L Number	Hits	Search Text	DB	Time stamp
1	23746	data with protection	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 16:54
2	493	(data with protection) and (key with hash)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 16:55
3	30	((data with protection) and (key with hash)) and (trust$2 with platform)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 17:04
4	1	016700.apn.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 17:01
5	25	(((data with protection) and (key with hash)) and (trust$2 with platform)) and (rsa with key)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 17:02
6	0	((((data with protection) and (key with hash)) and (trust$2 with platform)) and (rsa with key)) and (migrat$4 with key)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 17:04
7	688	(migrat$4 with key)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 17:17
8	14	((migrat$4 with key)) and (trust$2 with platform)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 17:13
9	5	(((migrat$4 with key)) and (trust$2 with platform)) and (tree or hierarchy)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 17:13
10	10	((migrat$4 with key)) and (trust$2 with computer)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 17:13
11	3	(((migrat$4 with key)) and (trust$2 with computer)) and (tree or hierarchy)	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 17:13
12	10	(migrat$4 with key) and (707/100).ccls.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 17:33
13	17	(secret$4 with key) and (707/100).ccls.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 17:19
14	19734	"14" and trust$	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 17:19

15	9	((secret$4 with key) and (707/100).ccls.) and trust$	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 17:19
16	993	(transfer$ with key) and trust$	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 17:34
17	299	((transfer$ with key) and trust$) and lock$3	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 17:34
18	230	(((transfer$ with key) and trust$) and lock$3) and decrypt$	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 17:36
19	14	((((transfer$ with key) and trust$) and lock$3) and decrypt$) and (key with (tree or hierarchy))	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/05/05 17:36

Google Web Images Groups News Froogle[New!] more »
related:islab.oregonstate.edu/documents/TCP Search Advanced Search Preferences

Web Results **21** - **21** of about **31** similar to **islab.oregonstate.edu/documents/TCPA/tpmpp%20v045.pdf**. (0.

Oregon State University Department of Mathematics
OSU Logo. Welcome to the Mathematics Department website. Math Midterm Schedule. Spring 2004 Colloquia. 19th Annual Lonseth Lecture (to ...
oregonstate.edu/Dept/math/ - 8k - Cached - Similar pages

In order to show you the most relevant results, we have omitted some entries very similar to the 21 already displayed.
If you like, you can repeat the search with the omitted results included.

◀ Gooogle
Result Page: **Previous** 1 2 3

related:islab.oregonstate.edu/docum Search

Language Tools | Search Tips

Google Home - Advertising Programs - Business Solutions - About Google

TCPA TPMPP

Version 0.45

Thu Sep 14 16:08:30 PDT 2000

Prepared By: David Grawrock

Prepared For: TCPA membership

TCPA Security Policy

Foreword

Before the Table of Contents there should be a foreword stating:

a) the reason for the PP,

b) where to send comments for the PP,

c) a revision history of the PP,

d) what authority the PP has, if any (e.g., A DoD standard, an NSA standard, an ANSI standard) and what communities (if any) are referencing the PP.

Table Of Contents

Item

List of Tables

Item

Conventions and Terminology

Conventions

Provide a description of any unique conventions to this document.

Terminology

Security Attributes – The security attributes are:

- **Migration** – The **migration** attribute determines if the entity can migrate from one TPM to another.
- Creation – The creation attribute indicates the creation status of an entity. Internal indicates that the entity creation occurred in the TPM external indicates that the entity came from outside the TPM.

- Type – The type attribute indicates if the entity is a signature **key**, encryption **key** or storage entity.

Document Organisation

Section 1 provides the introductory material for the **protection** profile

Section 2 provides general purpose and TOE description

Section 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware or software or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively, that must be satisfied by the TOE.

Section 6 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next Section 6 provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the **protection** profile requirements

An acronym list is provided to define frequently used acronyms.

A reference section is provided to identify background material.

1 - Introduction

Provide document management and overview information necessary to operate a **protection** profile registry. The Introduction should provide background information that enables the reader to gain a high-level understanding of the **protection** profile.

1.1 - Identification

Version Number: Draft Version 0.45

Registration:

A glossary of terms used in the **protection** profile (PP) is given in Annex B. This **protection** profile is hereafter referred to as the Trusted Computing Platform Alliance Trusted Platform Module **Protection** Profile (TCPA-TPMPP)

This PP has been built with Common Criteria (CC) Version 2.1 (ISO/IEC 15408) and Common Methodology for Information Technology Security Evaluation (CEM) 99/008 Version 0.6 January 1999.

The structure for this PP uses the Common Criteria Toolbox (Version 5.0i, 16 Feb 2000). This toolbox was developed by SPARTA, Inc., for the US National Security Agency. It is available through http://cctoolbox.sparta.com.

A product compliant with this PP may offer security features and functionality beyond that specified in this PP.

1.2 - Protection Profile Overview

This PP describes the IT security requirements for a security module known as the Trusted Platform Module (TPM). The TPM requires support from BIOS and software. The name in use for the supporting BIOS and software is Trusted Platform Subsystem (TPS) The security requirements in this PP apply to the TPM as shipped from the final assembly point of the TPM. The requirements in the TPMPP cover any hardware devices and firmware that create a TPM. There is no coverage for any entities in the TPS.

A separate PP known as the TCPA Trusted Platform Subsystem **Protection** Profile (TCPA-TPSPP) provides coverage for the TPS.

This PP does not target specific applications that use the TPM. Application coverage is at the operating system level would require a PP that provides coverage for an operating system.

The TPM is a collection of hardware and software. The mixture of hardware and software is a design feature for the manufacturer. The TCPA specification identifies "protected capabilities" and "protected data". The TPM is the module that provides the functionality and storage for the protected capabilities and protected data. All other features and data are part of the TPS. The TPMPP defines what is appropriate **protection** and how to evaluate the protections in the manufacturers design. The goal is to allow purchasers of various implementations of a TPM to compare the products using the same criteria.

The TPM will be the TOE. The TPM in all implementations will require significant help from the environment to properly provide a complete security solution. In particular, the TPM requires significant help in authentication and resource utilization.

The TPM provides security primitives in a secure environment. The primitives will include digital signatures, random number generation, protected storage and binding information to the TPM.

While the TPMPP makes no requirements on having hardware protections in the creation of a TPM subsystem, if hardware protections are not present then sufficient protections in the

environment must be present. For example, if the TPM were a software module of an A1 rated system (using the old Rainbow series) then the **protection** provided by the environment might meet the requirements.

TPM example

This definition is an example of one method of creating a TPM. Manufacturers may pick different ways of creating a TPM that are still compliant with the TPMPP.

For hardware TPM device, the TPM may be a computer chip embedded into a carrier. The chip is a semiconductor (silicon) integrated circuit (IC) fabricated in a complex microelectronic process, which involves repeatedly masking and doping the surface of a silicon substrate to form transistors, followed by patterning metal connections, and applying a protective overcoat. This process eventually yields a design comprising typically several hundred thousand transistors. The design consists of a central processing unit, an optional coprocessor, input and output lines, and volatile and non-volatile memory.

The chip will also be designed to be secure. In order to be secure, it should make appropriate use of both specific security enforcing design features, e.g. environmental sensors, and also technological properties of the materials and processes used.

A part of the manufacturing process is the inclusion of operating system (OS) developer-specific code, written in the microprocessor's native or machine code. This is usually contained in one of the numerous masks used during manufacture, referred to in this document as the ROM mask.

Requirement Summary

Functionality

The TCPA-TPMPP system targets these users needs –

- Providing a source of random numbers
- Providing a secure mechanism to perform the protected capability operations
- Providing a secure area to store the shielded data
- Providing mechanisms to store keys (both symmetric and asymmetric) that are useable only by the TPM
- Providing mechanisms to store integrity metrics
- Providing mechanisms to report on the integrity metrics
- Providing mechanisms to bind information to the TPM

- Providing mechanisms to manage the subsystem
- Providing resistance to resource depletion by providing resource allocation features
- Providing mechanisms to detect some insecurity
- Providing mechanisms for trusted recovery in the event of some system failures or detected insecurities
- Supporting these capabilities in a distributed system connected via an untrusted network

The TCPA-TPMPP is not expected to require that the TOE –

- Adequately protect against malicious abuse of authorized privileges.

- Adequately protect against sophisticated attacks (to include denial-of-service).
- Adequately protect against sophisticated hardware attacks (chip peeling etc.).
- Provide sufficient **protection** against installation, operation or administration errors.

Assurance

The TPMPP assurances are to provide a level of confidence resulting from existing best known methods of hardware and software development and no extensive third-party evaluation.

Assurance Level

The assurance level for this **protection** profile is EAL3.

Strength of function is medium.

Related Standards and Documents

- ISO 15408 - Information Technology - Security Techniques - Evaluation Criteria for IT Security (Hereafter referred to as "Common Criteria")
- Common Methodology for Information Security Evaluation (CEM) Version 0.6, 99/008, January 1999

Related Protection Profiles and Documents

Related Protection Profiles and Documents

PP Organization

The main sections of the PP are the TOE (target of evaluation) Description, TOE Security Environment, Security Objectives, IT Security Requirements, and Rationale.

The TOE Description provides general information about the TOE, serves as an aid to understanding its security requirements, and provides context for the PP's evaluation.

The TOE Security Environment describes security aspects of the environment in which the TOE is to be used and the manner in which it is to be employed. The TOE security environment includes:

a) Assumptions regarding the TOE's intended usage and environment of use

b) Threats relevant to secure TOE operation

c) Organizational security policies with which the TOE must comply

The security objectives reflect the stated intent of the PP. They pertain to how the TOE will counter identified threats and how it will cover identified organizational security policies and assumptions. Each security objective is categorized as being for the TOE or for the environment.

The Security Requirements section provides detailed requirements, in separate subsections, for the TOE and its environment.

The IT security requirements are subdivided as follows:

a) TOE Security Functional Requirements

b) TOE Security Assurance Requirements

TCPA Security Policy

The Application notes contain additional supporting information on issues unique to smart cards, consideration of management functions, and suggestions for the application of this PP through the use of packages applying to the basic chip, operating software, and integrated platform.

The Rationale presents evidence that the PP is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment.

The Rationale is in two main parts. First, a Security Objectives Rationale demonstrates that the stated security objectives are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them. Then, a Security Requirements Rationale demonstrates that the security requirements (TOE and environment) are traceable to the security objectives and are

suitable to meet them.

2 - TOE Description

Overview

The target of evaluation (TOE) is the integrated circuit and operating software, including the BIOS, of Trusted Platform Module (TPM). The security requirements in this **protection** profile apply to the TPM and it's software, from it's manufacture, to it's delivery to the motherboard manufacturer, to the platform manufacturer and finally to the end user.

Definition of TOE

Trusted Platform Module in this PP applies to the mechanism that provides the protected capabilities and shielded locations. The TPM could be an integrated circuit (IC) with non-volatile memory and a microprocessor or it could be a software module in a high assurance environment.

The TOE for the TPM must provide the assurances that the protected capabilities work properly and that the shielded locations properly shield the data.

Technology

There are a variety of technology issues relating to the TPM, which must be clearly delineated in a TCPA-TPMPP compliant product. These include implementation of security functions, attachment to motherboard and non-volatile memory.

Security functions

Many security relevant functionalities can be implemented in hardware or software or a combination of the two. This **protection** profile does not mandate how this functionality is to be implemented. Any Security Target claiming compliance with this **protection** profile should indicate how the required functionality is met.

Motherboard attachment

The TPM device must attach to the motherboard in some manner. The exact manner of attachment is left to the motherboard manufacturer. The manner of attachment must be reported

to any challenger when the TPM is in operation. This allows the challenger to make a trust decision based on how the TPM is attached to the motherboard.

Non-volatile memory

The type and amount of non-volatile memory available in the IC of the TPM must be reportable in a verifiable manner.

Cryptography

A variety of cryptographic keys are in use with the TPM, including endorsement keys, identity keys, transport keys and wrapping keys. Handling of these keys must be done in accordance with the **key** management procedures of this PP.

Cryptography may be implemented in hardware or software, with various algorithms and various **key** lengths. Some cryptographic operations must be performed on the IC with no secret data ever leaving the IC package. Other operations may perform operations with secret data off the IC package and in the software stack.

Any TOE claiming compliance with this **protection** profile must handle cryptographic functions in accordance with applicable international, industrial or organizational policies.

Required security functionality

TCPA-TPMPP specifies the requirements for a system with the security functionality listed below.

- Generating a random number
- Digitally signing a supplied value
- Storing a **key**
- Binding information to the subsystem
- Collecting integrity metrics
- Responding to requests regarding the state of the integrity metrics
- Auditing in support of individual accountability and detection of and response to insecurity
- Resource allocation features providing a measure of resistance to resource depletion
- Mechanisms for detecting some insecurities
- System recovery features providing a measure of survivability in the face of system failures and insecurities
- Automated support to help in the verification of secure delivery, installation, operation, and administration

Environments

The TPM environment is highly variable. In general, the TPM is assumed to be in an uncontrolled environment with no guarantee of the TPM's physical security. This allows TPM devices to be in mobile devices that are left in hotel rooms. The addition of physical security to the TPM device, on a server in a locked room, adds to the trust a challenger can make regarding the TPM

Attacker capabilities

Attackers are assumed to have various levels of expertise, resources, and motivation. Relevant expertise may be in general semiconductor technology, software engineering, hacking techniques or the specific TOE. Resources may range from personal computers to very expensive and sophisticated engineering test and measurement devices. They may also include software routines, some of which are readily available on the Internet. Motivation may include economic reward or the satisfaction and notoriety of defeating expert security. It is assumed that given sufficient time and expertise, any TPM can be compromised.

TOE identification

Through selection of the ACM Configuration Management Class of assurance functions this PP imposes the requirement that a unique reference be utilized to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labeling the TOE with this reference then ensures that users of the TOE can be aware of which instance of the TOE they are using. The TOE described herein is, however, a combination of hardware and software, each portion of which may be composed of a further collection of components. This aggregate collection offers the potential for confusion in identifying a unique reference for the TOE.

To further complicate identification, commonly an IC can be produced with multiple features, only some of which are enabled. The design layout of the IC (the photomask) determines the functionality; however, as fabrication technology improves, the identical design may be used to produce an otherwise identical chip but with a reduced feature size. Likewise, software features may be selectively employed, depending on hardware functions. However, the presence or absence of specific features may directly contribute to the possible introduction of vulnerabilities. For example, the size of the IC features is directly related to the relative difficulty of probing. A potentially unknown, but present, software feature may allow backdoors or other routes for penetration.

It is therefore essential that the unique reference for the TOE compliant with this PP allow the identification of at least

- The microprocessor specification
- The memory size and allocation (ROM, EEPROM, RAM, etc.)
- The physical instantiation of the IC design regarding layout and feature size
- All hardware security features on the IC, whether they are initially enabled or not
- All enabled hardware security features
- The connection of the TPM to the motherboard
- The software specification
- All software security features present, whether they are initially enabled or not
- All enabled software security features

The TOE Description is a critical part of the **protection** profile. Provide a TOE description that enables the reader to:
(1) gain an understanding of how the system operates,
(2) know where the component fits into the system, and
(3) be able to define the TOE operation and its limitations. Be sure to include at least one figure that shows

the relationship of the TOE elements or shows the relationship of the TOE to its environment.

3 - TOE Security Environment

Summarise the security environment in which the TOE will be used and the manner the TOE will be employed.

3.1 - Secure Usage Assumptions

A.Application_use: TOE application use

The TOE will be in use in various applications (i.e. data storage, binding to platform, system integrity and others) to provide security services and protect sensitive information.

A.Configuration: TPM configuration

The TOE will be properly installed and configured.

A.Conformance: Confomance guarantee

The use of the TOE does not guarantee the security of the overall system. The TPM is a subsystem and requires signficant support from the environment to provide a total security solution. The platform manufacturer and end user must provide the environmental security appropriate to the data functions that must be protected.

A.Hostile_User: Hostile users

Users cannot be trusted and are considered to be hostile.

A.Outsider_Med: Proficient threat agents

The TOE is subject to deliberate attack by threat agents proficient in the security behavior of the system.

A.Physical: Physical attack

The TOE is assumed to be protected from physical tampering through features and technologies.

A.System: System description

The TOE is assumed to be a subsystem of a computing platform that provides OS, storage, input/output to TOE and TOE utilization functions.

A.TCPAIdentityCertification: Identity Certification

The TOE requires outside help to certify identities.

A.TCPARootMeasurement: TCPA Root of measurement trust
The TPS will supply the root of measurement trust.

A.Trusted_User: Trusted users
Authorized users are trusted not to compromise security.

3.2 - Threats to Security

T.Admin_Err_Commit: Administrative errors of commission
An administrator commits errors that directly compromise organizational security objectives or change the technical security policy enforced by the system or application.

T.Admin_Err_Omit: Administrative errors of omission
The system administrator fails to perform some function essential to security.

T.Admin_UserPriv: Administrator violates user privacy policy
An administrator learns the identity (or other privacy related information) of user(s) in violation of user privacy policy. Privacy-related information is sensitive information associated with the identity of a user.

T.Component_Failure: A critical system component fails
Failure of one or more system components results in the loss of system-critical functionality.

T.Dev_Flawed_Code: Software containing security-related flaws
A system or applications developer delivers code that does not perform according to specifications or contains security flaws.

T.EndorseExpose: Exposure of endorsement **key**
The endorsement **key** provides the root of reporting trust. If exposed it provides the attacker numerous mechanisms that allow for the forgery, cloning and masquerading as a valid TPM

T.Failure_DS_Comp: Failure of a distributed system component
Failure of a component that is part of a distributed system will cause other parts of the distributed system to malfunction or provide unreliable results.

T.GlobalSecret: Global secret exposure
If the TOE has a global secret known to all TOE's then exposure of one TOE exposes all TOE's.

T.Hack_AC: Hacker undetected system access

A hacker gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.

T.Hack_Avl_Resource: Hacker attempts resource denial of service
A hacker executes commands, sends data, or performs other operations that make system resources unavailable to system users. Resources that may be denied to users include bandwidth, processor time, memory, and data storage.

T.Hack_Comm_Eavesdrop: Hacker eavesdrops on user data communications
Hacker obtains user data by eavesdropping on communications lines.

T.Hack_Crypto: Cryptoanalysis for theft of information
A hacker performs cryptoanalysis on encrypted data in order to recover message content.

T.Hack_Msg_Data: Message content modification
A hacker modifies information intercepted from a communication link between two unsuspecting entities before passing it on, thereby deceiving the intended recipient.

T.Hack_Phys: Exploitation of vulnerabilities in the physical environment of the system
A hacker physically interacts with the system to exploit vulnerabilities in the physical environment, resulting in arbitrary security compromises.

T.Hack_Social_Engineer: Social engineering
A hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation.

T.IdenClone: Identity cloning
Identities are unique keys that must remain protected by the TPM. Creating a copy of the identity breaks the uniqueness promise.

T.IdenPKI: Identity PKI

The identity creation process requires a PKI to certify the identity. This PKI must ensure the uniqueness of the identity and validate the endorsement **key**. Failure to properly perform these operations results in a bad identity.

T.Malicious_Code: Malicious code exploitation
An authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of system assets.

T.MeasureFalse: False integrity measurement
The entity or process providing the integrity measurement provides a false value.

T.OwnerMasquerade: Owner masquerade
At attacker can masquerade as the owner of either the TPM or an entity if they obtain the owner authorization data.

T.Power_Disrupt: Unexpected disruption of system or component power
A human or environmental agent disrupts power causing the system to lose information or security **protection**.

T.ProtStorAttribute: Protected storage attribute
Each protected storage object has attributes that indicate it's **migration** status, object type and source. Modification of these attributes allows the attacker to use the object in an unauthorized manner.

T.ProtStoreBackup: Protected storage backup
The protected storage backup mechanism must provide assurances that the **migration** and non-**migration** bits are properly followed. If they are not followed then non-**migratable** information may move from one system to another.

T.ProtStoreCrypto: Protected Storage Cryptography
Protected storage requires cryptography to protect the contents when the data is not inside

Protected storage requires cryptography to protect the contents when the data is not inside the TPM. Failure of the cryptography exposes the data.

T.ProtStoreMaintenance: Protected storage maintenance
The protected storage maintenance feature allows for the cloning of a TPM. If this mechanism is abused then the attacker can make copies of TPM devices.

T.Repudiate_Receive: Recipient denies receiving information
The recipient of a message denies receiving the message, to avoid accountability for receiving the message or to avoid obligations incurred as a result of receiving the message.

T.Repudiate_Send: Sender denies sending information
The sender of a message denies sending the message to avoid accountability for sending the message or to avoid obligations incurred as a result of sending the message.

T.Repudiate_Transact: A participant denies performing a transaction
A participant in a transaction denies participation in the transaction to avoid accountability for the transaction or for resulting obligations.

T.SpecRef: Failure to follow specification
The developer creating the TOE does not follow the TCPA specification and makes mistakes in implementation. This creates holes in the TOE that expose user and internal information.

T.Spoofing: Legitimate system services are spoofed
An attacker tricks users into interacting with spurious system services.

T.User_Abuse_Conf: Hostile user acts cause confidentiality breaches
A user collects sensitive or proprietary information and removes it from the system.

T.User_Collect: User abuses authorization to collect data
User abuses granted authorizations to improperly collect sensitive or security-critical

data.

T.User_Err_Conf: User errors cause confidentiality breaches
A user commits errors that cause information to be delivered to the wrong place or wrong person.

T.User_Err_Inaccess: User error makes data inaccessible
A user accidentally deletes user data or changes system data rendering user data inaccessible.

T.User_Err_Integrity: User errors cause integrity breaches
A user commits errors that induce erroneous actions by the system and/or erroneous statements its users.

T.User_Err_Slf_Protect: User errors undermine the system's security features
A user commits errors that cause the system or one of its applications to undermine the system's security features.

T.User_Misuse_Avl_Resc: User's misuse causes denial of service
A user's unauthorized use of resources causes an undue burden on an affected resource.

T.User_Modify: User abuses authorization to modify data
A user abuses granted authorizations to improperly change or destroy sensitive or security-critical data.

T.User_Send: User abuses authorization to send data
A user abuses granted authorizations to improperly send sensitive or security-critical data.

3.3 - Organisational Security Policies

P.Accountability: Individual accountability
Individuals shall be held accountable for their actions.

P.Authorities: Notification of threats and vulnerabilities
Appropriate authorities shall be immediately notified of any threats or vulnerabilities impacting systems that process their data.

P.Availability: Information availability
Information shall be available to satisfy mission requirements.

P.EMI_EMC: EMI Emissions
The TOE security policy must specify what level of emissions are permissable when the

TOE executes cryptographic operations.

TCPA Security Policy

P.Guidance: Installation and usage guidance
Guidance shall be provided for the secure installation and use of the system.

P.Information_AC: Information access control
Information shall be accessed only by authorized individuals and processes.

P.Integrity: Information content integrity
Information shall retain its content integrity.

P.Lifecycle: System lifecycle phases integrate security
Information systems security shall be an integral part of all system lifecycle phases.

P.Marking: Information marking
Information shall be appropriately marked and labeled.

P.MessageAuth: Message authorization
Each message to a TPM protected capability uses the authorization protocol

P.Physical_Control: Physical **protection**
Information shall be physically protected to prevent unauthorized disclosure, destruction, or modification.

P.SpecRef: Specification reference
The TOE must provide all features and functions of the TCPA in a consistent manner.

P.TCPAAuthorization: TCPA Authorization
The TOE must provide the ability to participate in the authorization protocol from chapter 4.

P.TCPAIdentities: TCPA Identities
The TOE must create and manage identities.

P.TCPAOwnership: TCPA TPM and entity ownership
The TOE must provide the mechanisms to create and use the ownership protocol.

P.TCPAProtectMigrate: TCPA Protected storage **migration** and non **migration**
The TOE must provide the mechanisms to identity the **tree** a storage entity is in (**migratable** or non-**migratable**), ensure that the label once set never changes and manage the **migration**, backup and recovery of storage entities.

P.TCPARegDIR: TCPA DIR registers
The TOE must supply DIR registers.

P.TCPARegPCR: TCPA PCR registers
The TOE must provide volatile PCR registers

P.TSP: TOE Security Policy
A TOE security policy (TSP) must identify all roles, services and security relevant data items, and specify what access (if any) a user, performing a service within the context of a given role, has to each of the secuiryt-relevant data items. The policy must specify that: users agree to protect keys and data access, users agree to report loss of keys or perceived compromise to security and user agree not to collude.

4 - Security Objectives

Identify and define the security objectives for the TOE and its environment. Security objectives should reflect the stated intent, be suitable to counter all identified threats, and cover all identified organisational securitypolicies and assumptions.

4.1 - Security Objectives for the TOE

O.AC_Label_Export: Object security attributes and exportation

O.AC_Label_Export: Object security attributes and exportation
Provide object security attributes in exported data with moderate to high effectiveness. The attributes are those associated with specific security function policies.

O.Admin_Code_Val: Administrative validation of executables
Validate executable objects prior to allowing execution. Validation needs to be done by someone with an expertise to recognize malicious code and the authority and means to prevent its execution.

O.Admin_Guidance: Administrator guidance documentation
Deter administrator errors by providing adequate administrator guidance.

O.Apply_Code_Fixes: Apply patches to fix the code
Apply patches to fix the code when vulnerabilities in code allow unauthorized and undiscovered access.

O.Atomic_Functions: Complete security functions or recover to previous state
Recover automatically to a consistent, secure state if a security function does not complete successfully in the presence of certain types of failures.

O.AuditLog: Audit Log
The TPS shall maintain the audit log

O.Audit_Generation: Audit records with identity
Record in audit records: date and time of action, location of the action, and the entity responsible for the action.

O.Change_Control_Users: User notification of data content changes
Notify users of changes to data content in order to make any adjustments to their own data.

O.Clean_Obj_Recovery: Object and data recovery free from malicious code

Recover to a viable state after malicious code is introduced and damage occurs, removing the malicious code as part of the process.

O.Code_Signing: Code signing and verification.
Check verification of signed downloaded code prior to execution. A well-known example is checking digital signatures on signed Java applets.

O.Config_Management: Implement operational configuration management
Implement a configuration management plan. Implement configuration management to assure storage integrity, identification of system connectivity (software, hardware, and firmware), and identification of system components (software, hardware, and firmware).

O.Crypto_AC: Cryptographic access control policy
Restrict user access to cryptographic IT assets in accordance with a specified user access control policy.

O.Crypto_Data_Sep: Separation of cryptographic data
Provide complete separation between plaintext and encrypted data and between data and keys. This requires separate channels and separate storage areas. The only place any data can pass between the plaintext and encrypted data modules is in the cryptographic engine. There should be no way for plaintext keys to reach either data module and no way for data to enter the **key** handling module. Eencrypted keys can be handled as encrypted data, but with limited user access.

O.Crypto_Dsgn_Impl: Cryptographic Design and Implementation
Minimize or even eliminate design and implementation errors in the cryptographic modules and functions.

O.Crypto_Import_Export: Cryptographic import, export, and inter-TSF transfer
Protect cryptographic data assets when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users.

O.Crypto_Key_Man: Cryptographic **Key** Management
Fully define cryptographic components, functions, and interfaces. Ensure appropriate **protection** for cryptographic keys throughout their lifecycle, covering generation, distribution, storage, use, and destruction.

O.Crypto_Modular_Dsgn: Cryptographic Modular Design
Prevent errors in one part of the TOE from influencing other parts, especially cryptographic parts. To this end, noncryptographic I/O paths must be well defined and

logically independent of circuitry and processes performing **key** generation, manual **key** entry, **key** zeroising, and similar **key**-related operations.

O.Crypto_Operation: Cryptographic function definition
Cryptographic components, functions, and interfaces shall be fully defined.

O.Crypto_Self_Test: Cryptographic self test
Provide the ability to verify that the cryptographic functions operate as designed.

O.Crypto_Test_Reqs: Test cryptographic functionality
Test cryptographic operation and **key** management.

O.Data_Exchange_Conf: Enforce data exchange confidentiality
Protect user data confidentiality when exchanging data with a remote system.

O.Data_Export_Control: Control user data exportation
Impose information control policies that do not allow export of specified data and/or export to specified locations.

O.Data_Imp_Exp_Control: Data import/export to/from system control
Protect data from being sent to erroneous places and more places external to the system than allowed by the organization's security policy. Conversely the import of data into the system should be protected from illicit information or information not allowed by the organization's security policy.

O.EMSEC_Design: Provide physical emanations security
Design and build the system in such a way as to control the production of intelligible emanations within specified limits.

O.Export_Control: Sanitize data objects containing hidden or unused data
Sanitize data objects that may contain hidden data when they are exported from the TOE in order to inhibit steganographic smuggling.

O.External_Labels: Label or mark information for external systems
Label or mark information for external systems to prevent the exchange of inappropriate

data between systems.

O.Fail_Secure: Preservation of secure state for failures in critical components
Preserve the secure state of the system in the event of a secure component failure.

O.Fault_Tolerance: Provide fault tolerant operations for critical components
Provide fault tolerant operations for critical components and continue to operate in the presence of specific failures in one or more system components.

O.General_Integ_Checks: Periodically check integrity
Provide periodic integrity checks on both system and user data.

O.Hack_Limit_Sessions: Limit sessions to outside users
Limit the number of sessions available to outside users. A hacker can initiate multiple communication sessions that could cause an overload on resources, for example, half open session starts as is seen in "SYN flood" attacks.

O.Info_Flow_Control: System enforced information flow
Enforce an information flow policy whereby users are constrained from allowing access to information they control, regardless of their intent (e.g., mandatory access control). This lattice property of security attributes is commonly associated with the U.S. DoD implementations of Mandatory Access Control (MAC).

O.Input_Inspection: Require inspection for absence of malicious code.
Require inspection of downloads/transfers.

O.Integ_Data_Mark_Exp: Data marking integrity export
Ensure that data markings are included with data that is exported to another trusted product.

O.Integ_Sys_Data_Ext: Integrity of system data transferred externally
Ensure the integrity of system data exchanged externally with another trusted product by using a protocol for data transfer that will permit error detection and correction. This includes detecting and possibly correcting errors in data received and encoding

This includes detecting and possibly correcting errors in data received and encoding

outgoing data to make it possible for the receiver to detect and possibly correct errors. The method for detecting and correcting errors is based on some method (protocol) that is agreed upon by participating parties.

O.Integ_Sys_Data_Int: Integrity of system data transferred internally
Ensure the integrity of system data transferred internally.

O.Integ_User_Data_Int: Protect user data during internal transfer
Ensure the integrity of user data transferred internally within the system.

O.Integrity_Data/SW: Integrity **protection** for user data and software
Provide integrity **protection** for user data and software.

O.Integrity_Data_Rep: Integrity of system data replication
Ensure that when system data replication occurs across the system the data is consistent for each replication.

O.Integrity_Practice: Operational integrity system function testing
Provide system functional tests to periodically test the integrity of the hardware and code running system functions.

O.IntelEman_Contain: Emanations containment
Confine system-produced intelligible emanations to within a specified limit.

O.IntelEman_Control: Emanations control
Limit system-produced intelligible emanations to within a specified limit.

O.Lifecycle_Security: Lifecycle security
Provide tools, techniques, and security employed during the development phase. Detect and resolve flaws during the operational phase. Provide safe destruction techniques.

O.Limit_Actions_Auth: Restrict actions before authentication

Restrict the actions a user may perform before the TOE verifies the identity of the user.

O.Limit_Comm_Sessions: Limit the number of user initiated communication sessions
Provide mechanisms to limit the number of sessions that the user can initiate, if the user initiates multiple sessions that exceed the processors ability to perform in a reliable and efficient manner. These sessions could ether be communication (TCP/IP) sessions or user login sessions.

O.Maintain_Sec_Domain: Maintain security domain
Maintain at least one security domain for system (TOE) execution to protect the TOE from interference and tampering.

O.Malicious_Code: Procedures for preventing malicious code
Incorporate malicious code prevention procedures and mechanisms.

O.Manage_Res_Sec_Attr: Manage resource security attributes
Provide management on resource security attributes.

O.Manage_TSF_Data: Manage security-critical data to avoid storage space being exceeded
Manage security-critical (TSF) data to ensure that the size of the data does not exceed the space allocated for storage of the data.

O.MessageAuthentication: Message authentication
Each requestor must prove knowledge of the shared secret.

O.MetricReporting: Integrity metric reporting
The TOE must report the values in the current PCR registers. The report may be digitally signed.

O.NoBore: No BORE attacks
The TOE provides **protection** from Break Once Run Everywhere attacks.

O.No_Residual_Info: Eliminate residual information
Ensure there is no "object reuse;" i.e., ensure that there is no residual information in some information containers or system resources upon their reallocation to different users.

O.NonRepud_Assess_Recd: Non-repudiation support for received information by a nonlocal sender's TSF
Support nonrepudiation for received information by supporting remote handling of nonrepudiation evidence if needed.

O.NonRepud_Assess_Sent: Non-repudiation support for sent information by the nonlocal receiving TSF.
Support nonrepudiation for sent information by supporting remote handling of nonrepudiation evidence if needed.

O.NonRepud_Gen_Recd: Non-repudiation support for received information by the recipient's TSF
Prevent a receiving user from avoiding accountability for receiving a message by providing evidence that the user received the message.

O.NonRepud_Gen_Sent: Non-repudiation support for sent information by the sender's TSF.
Prevent a user from avoiding accountability for sending a message to a recipient at a different site by providing evidence that the user sent the message.

O.Obj_Attr_Integrity: Basic object attribute integrity
Maintain object security attributes with moderate to high accuracy (under the guidance of qualified users).

O.Obj_Protection: Object domain **protection**
Require domain **protection** for objects. Specify object classes (domains), user groups, and operation classes. Use these to specify which operations may be performed on which objects by which users. Basically this controls what users can do in a given group.

O.Prevent_Link: Prevent linking of multiple service use
Ensure that a user may make multiple uses of a service or resource without other specified users being able to link these uses together.

O.Protected_Capability: Protected Capability and shielded location
The TOE must identity and protect capabilities as defined in the TCPA specification.

O.Rcv_MsgMod_ID: Identify message modification in messages received
The TSF recognizes changes to messages that occurred in transit, including insertion of spurious messages and deletion or replay of legitimate messages.

spurious messages and deletion or replay of legitimate messages.

O.React_Discovered_Atk: React to discovered attacks
Implement automated notification or other reactions to the TSF-discovered attacks in an effort to identify attacks and to create an attack deterrent.

O.RootMeasurement: Measurement root of trust
The entity that provides the base for measuring integrity values is the measurement root of trust. This entity on a PC would be the boot block or something similar.

O.RootReporting: Reporting root of trust
The reporting root of trust is the endorsement **key**. This provides a singular point that all challengers can rely on.

O.SecureManufacturing: Secure TPM creation and certification
The TPM manufacturing process requires the creation and certification of the endorsement **key**. The TPM manufacturing process must perform this creation and certification in a manner that provides the assurances that the endorsement **key** was properly created. The process must also provide assurances that the certification of the endorsement **key** is done with the correct private **key** and that the process protects the certfication **key** and properly protects certfication process.

O.Secure_State: Protect and maintain secure system state
Maintain and recover to a secure state without security compromise after system error or other interruption of system operation.

O.Security_Attr_Mgt: Manage security attributes
Manage the initialization of, values for, and allowable operations on security attributes.

O.Security_Data_Mgt: Manage security-critical data
Manage the initialization of, limits on, and allowable operations on security-critical data.

Manage the initialization of, limits on, and allowable operations on security-critical data.

O.Security_Func_Mgt: Manage behavior of security functions
Provide management mechanisms for security mechanisms.

O.Security_Roles: Security roles
Maintain security-relevant roles and the association of users with those roles.

O.Snt_MsgMod_ID: Identify message modification in messages sent
The TSF supports recognition of changes to transmitted messages that occurred in transit, including insertion of spurious messages and deletion or replay of legitimate messages.

O.Source_Code_Exam: Examine the source code for developer flaws
Examine for accidental or deliberate flaws in code made by the developer. The accidental flaws could be lack of engineering detail or bad design. Where the deliberate flaws would include building trapdoors for later entry as an example.

O.SpecRef: Specification reference
The TOE must provide all of the features and functions as specified in the TCPA specification.

O.Standard_Output_Pres: Standard presentation of output values
Present each possible output value in a standard form.

O.Storage_Integrity: Storage integrity
Provide integrity for data.

O.Sys_Assur_HW/SW/FW: Validation of security function
Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures.

O.Sys_Backup_Procs: System backup procedures

Provide backup procedures to ensure that the system can be reconstructed.

O.Sys_Backup_Verify: Detect modifications of backup hardware, firmware, software
Detect modifications to backup hardware, firmware, and software.

O.Sys_Self_Protection: **Protection** of system security function
Protect the system security functions through technical features.

O.TCPAIdentities: TCPA Identities
The TOE must provide the ability to create, manage and use identities.

O.TCPAProtectedStorage: TCPA Protective Storage
The TOE must provide a protected storage mechanism as defined in the specification section 3.6 and chapter 6.

O.TSF_Rcv_Err_ID_Loc: Local detection of received security-critical data modified in transit
Identification by the system (TOE) of modification of security-critical (TSF) data occurring in transit from a remote trusted site must occur.

O.TSF_Rcv_Err_ID_Rem: Remote detection of received security-critical data modified in transit
Identification by the remote site of the modification of security-critical (TSF) data occurring in transit from the remote site must occur.

O.TSF_Snd_Err_ID_Loc: Local detection of sent security-critical data modified in transit
Identification of modification of security-critical (TSF) data occurring in transit to a remote site by the TSF must occur.

O.TSF_Snd_Err_ID_Rem: Remote detection of sent security-critical data modified in transit.
Identification of modification of security-critical (TSF) data occurring in transit to a remote site by the remote site must occur.

O.Tamper_ID: Tamper detection
Provide system features that detect physical tampering of a system component, and use those features to limit security breaches.

O.Tamper_Resistance: Tamper resistance
Prevent or resist physical tampering with specified system devices and components.

O.Trusted_Path: Provide a trusted path
Provide a trusted path between the user and the system. Execution of a user-requested action must be made via a trusted path with the following properties:
* The path is logically distinct from, and cannot be confused with other communication paths (by either the user or the system).
* The path provides assured identification of its end points.

O.Trusted_Recovery: Trusted recovery of security functionality
Recovery to a secure state, without security compromise, after a discontinuity of operations.

O.Trusted_Recovery_Doc: Documentation of untrusted data recovery
Provide trusted recovery to ensure that data cannot be lost or misplaced. Any circumstances which can cause untrusted recovery to be documented with mitigating procedures established.

O.User_Auth_Management: User authorization management
Manage and update user authorization and privilege data in accordance with organizational security and personnel policies.

O.User_Conf_Prevention: Basic confidentiality-breach prevention
Prevent unauthorized export of confidential information from the TOE with moderate effectiveness.

O.User_Data_Integrity: Integrity **protection** of stored user data
Provide appropriate integrity **protection** for stored user data.

O.User_Data_Transfer: **Protection** of transmitted user data
Provide the ability to have physically protected communications lines, intrusion detection for communications lines, and/or need-to-know isolation for communications lines.

O.User_Defined_AC: User-defined access control
Enforce an access control policy whereby users may determine who may access information they control.

O.User_Guidance: User guidance documentation
Provide documentation for the general user.

Security Objectives:

4.2 - Security Objectives for the Environment

O.AuditLog: Audit Log
The TPS shall maintain the audit log

O.Audit_Protect: Protect stored audit records
Protect audit records against unauthorized access, modification, or deletion to ensure accountability of user actions.

O.Trusted_Path: Provide a trusted path
Provide a trusted path between the user and the system. Execution of a user-requested action must be made via a trusted path with the following properties:
* The path is logically distinct from, and cannot be confused with other communication paths (by either the user or the system).
* The path provides assured identification of its end points.

5 - IT Security Requirements

Include an overall summary of the functional and assurance security requirements for the TOE, and environment.

5.1 - TOE Security Functional Requirements

5.1.0.1 - Security alarms (FAU_ARP.1)

The TSF shall take Shutdown of TOE functions. upon detection of a potential security violation. FAU_ARP.1.1

5.1.0.2 - Audit data generation (FAU_GEN.1)

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the minimum level of audit; and

c) all protected capabilities per TCPA specification. FAU_GEN.1.1

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, parent entity FAU_GEN.1.2

5.1.0.3 - Selective audit (FAU_SEL.1)

The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) event type

b) none. FAU_SEL.1.1

5.1.0.4 - Selective proof of origin (FCO_NRO.1)

The TSF shall be able to generate evidence of origin for transmitted all authorized

The TSF shall be able to generate evidence of origin for transmitted all authorized commands per the TCPA spec at the request of the recipientnone. FCO_NRO.1.1
The TSF shall be able to relate the nonces of the originator of the information, and the command ordinal, security sensitive parameters as per TCPA specification of the information to which the evidence applies. FCO_NRO.1.2
The TSF shall provide a capability to verify the evidence of origin of information to recipientnone given evidence only available when requestor properly authenticates. FCO_NRO.1.3

5.1.0.5 - Enforced proof of origin (FCO_NRO.2)

The TSF shall enforce the generation of evidence of origin for transmitted all authorized commands per the TCPA spec at all times. FCO_NRO.2.1
The TSF shall be able to relate the nonces of the originator of the information, and the command ordinal, security sensitive parameters as per TCPA specification of the information to which the evidence applies. FCO_NRO.2.2
The TSF shall provide a capability to verify the evidence of origin of information to recipientnone given evidence only available when requestor properly authenticates. FCO_NRO.2.3

5.1.0.6 - Selective proof of receipt (FCO_NRR.1)

The TSF shall be able to generate evidence of receipt for received all authorized commands provide an authenticated return message at the request of the originatornone. FCO_NRR.1.1
The TSF shall be able to relate the nonces of the recipient of the information, and the command ordinal, return code, security sensitive parameters as per TCPA specification of the information to which the evidence applies. FCO_NRR.1.2
The TSF shall provide a capability to verify the evidence of receipt of information to originatornone given only available when the command properly authenticated, failures have no ability to provide evidence. FCO_NRR.1.3

5.1.0.7 - Enforced proof of receipt (FCO_NRR.2)

The TSF shall enforce the generation of evidence of receipt for received all authorized commands provide an authenticated return message. FCO_NRR.2.1

The TSF shall be able to relate the nonces of the recipient of the information, and the command ordinal, return code, security sensitive parameters as per TCPA specification of the information to which the evidence applies. FCO_NRR.2.2

The TSF shall provide a capability to verify the evidence of receipt of information to originatornone given only available when the command properly authenticated, failures have no ability to provide evidence. FCO_NRR.2.3

5.1.0.8 - Cryptographic key generation (FCS_CKM.1)

The TSF shall generate cryptographic keys in accordance with a specified cryptographic **key** generation algorithm P1363 and specified cryptographic **key** sizes RSA 512, 768, 1024, 2048 that meet the following: P1363, PKCS#1 V2. FCS_CKM.1.1

5.1.0.9 - Cryptographic key destruction (FCS_CKM.4)

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic **key** destruction method erasure of all memory areas that meets the following: P1363. FCS_CKM.4.1

5.1.0.10 - Cryptographic operation (FCS_COP.1)

The TSF shall perform RSA encrypt **decrypt**, SHA, HMAC in accordance with a specified cryptographic algorithm RSA, SHA, HMAC and cryptographic **key** sizes RSA 512, 768, 1024, 2048 that meet the following: P1363, PKCS#1 V2, RFC 2104, SHA. FCS_COP.1.1

5.1.0.11 - Complete access control (FDP_ACC.2)

The TSF shall enforce the Owner access control on TPM owner, all protected storage nodes, all identities and all operations among subjects and objects covered by the SFP. FDP_ACC.2.1

The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP. FDP_ACC.2.2

5.1.0.12 - Security attribute based access control (FDP_ACF.1)

The TSF shall enforce the TCPA ownership protocol to objects based on ownership token, protected storage attributes. FDP_ACF.1.1

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: i) entity use requires use authorization ii) entity loading requires authorization of entity owner. FDP_ACF.1.2

ii) entity loading requires authorization of entity owner.

The TSF shall explicitly authorise access of subjects to objects based on the following

additional rules: knowledge of ownership token authorizes access to entity. FDP_ACF.

The TSF shall explicitly deny access of subjects to objects based on the failure to provide ownership token. FDP_ACF.1.4

5.1.0.13 - Basic data authentication (FDP_DAU.1)

The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of BIND, SEAL and WRAP entities, endorsement and SRK keys, identities, FDP_DAU.1.1

The TSF shall provide TPM with the ability to verify evidence of the validity of the indicated information. FDP_DAU.1.2

5.1.0.14 - Export of user data with security attributes (FDP_ETC.2)

The TSF shall enforce the TCPA ownership protocol when exporting user data, controlled under the SFP(s), outside of the TSC. FDP_ETC.2.1

The TSF shall export the user data with the user data's associated security attributes. FDP_ETC.2.2

The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data. FDP_ETC.2.3

The TSF shall enforce the following rules when user data is exported from the TSC: none. FDP_ETC.2.4

5.1.0.15 - Complete information flow control (FDP_IFC.2)

The TSF shall enforce the TCPA flow control

on TCPA flow control controls

i) Endorsement **key**

ii) SRK

iii) protected storage nonces

iv) user data and all operations that cause that information to flow to and from subjects

covered by the SFP. FDP_IFC.2.1

The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP. FDP_IFC.2.2

5.1.0.16 - Simple security attributes (FDP_IFF.1)

The TSF shall enforce the TCPA flow control based on the following types of subject and information security attributes: i) creation location (on or off TPM)
ii) **migration** status
iii) load location (on or off TPM). FDP_IFF.1.1

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **migration** status must match, location must match. FDP_IFF.1.2

The TSF shall enforce the none. FDP_IFF.1.3

The TSF shall provide the following none. FDP_IFF.1.4

The TSF shall explicitly authorise an information flow based on the following rules: **migration** status match, TCPA backup, TCPA maintenance. FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: i) mismatch of **migration**
ii) mismatch of load location. FDP_IFF.1.6

5.1.0.17 - Import of user data without security attributes (FDP_ITC.1)

The TSF shall enforce the TCPA ownership protocol when importing user data, controlled under the SFP, from outside of the TSC. FDP_ITC.1.1

The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC. FDP_ITC.1.2

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: none. FDP_ITC.1.3

5.1.0.18 - Import of user data with security attributes (FDP_ITC.2)

The TSF shall enforce the TCPA ownership protocol when importing user data, controlled under the SFP, from outside of the TSC. FDP_ITC.2.1

The TSF shall use the security attributes associated with the imported user data.

The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received. FDP_ITC.2.3

The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data. FDP_ITC.2.4

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: none. FDP_ITC.2.5

5.1.0.19 - Transmission separation by attribute (FDP_ITT.2)

The TSF shall enforce the TCPA ownership protocol to prevent the disclosure modification of user data when it is transmitted between physically-separated parts of the TOE. FDP_ITT.2.1

The TSF shall separate data controlled by the SFP(s) when transmitted between physically-separated parts of the TOE, based on the values of the following: **migration** and end location. FDP_ITT.2.2

5.1.0.20 - Attribute-based integrity monitoring (FDP_ITT.4)

The TSF shall enforce the TCPA ownership protocol to monitor user data transmitted between physically-separated parts of the TOE for the following errors: changes to wrapped entity, based on the following attributes: **migration** attribute. FDP_ITT.4.1

Upon detection of a data integrity error, the TSF shall generate audit event, stop usage of object. FDP_ITT.4.2

5.1.0.21 - Subset residual information protection (FDP_RIP.1)

The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from the following objects: all loaded keys. FDP_RIP.1.1

5.1.0.22 - Full residual information protection (FDP_RIP.2)

The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from all objects. FDP_RIP.2.1

5.1.0.23 - Basic rollback (FDP_ROL.1)

The TSF shall enforce TCPA security policy to permit the rollback of the entity loading, entity wrapping, on the entities. FDP_ROL.1.1
The TSF shall permit operations to be rolled back within the before release of the entity to operation by other TPM functions. FDP_ROL.1.2

5.1.0.24 - Stored data integrity monitoring and action (FDP_SDI.2)

The TSF shall monitor user data stored within the TSC for integrity errors, **migration** status, TPM assignment on all objects, based on the following attributes: user data attributes. FDP_SDI.2.1
Upon detection of a data integrity error, the TSF shall rejection of load operation. FDP_SDI.2.2

5.1.0.25 - Basic data exchange confidentiality (FDP_UCT.1)

The TSF shall enforce the TCPA ownership protocol and TCPA flow control to be able to transmit objects in a manner protected from unauthorised disclosure. FDP_UCT.1.1

5.1.0.26 - Data exchange integrity (FDP_UIT.1)

The TSF shall enforce the TCPA flow control to be able to transmit user data in a manner protected from modification deletion insertion errors. FDP_UIT.1.1
The TSF shall be able to determine on receipt of user data, whether modification deletion insertion has occurred. FDP_UIT.1.2

5.1.0.27 - Authentication failure handling (FIA_AFL.1)

The TSF shall detect when 5 unsuccessful authentication attempts occur related to TPM owner, entity owner. FIA_AFL.1.1
When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall rejection of session, creation of audit event. FIA_AFL.1.2

5.1.0.28 - User authentication before any action (FIA_UAU.2)

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. FIA_UAU.2.1

5.1.0.29 - Single-use authentication mechanisms (FIA_UAU.4)

The TSF shall prevent reuse of authentication data related to ownership protocol from TCPA specification. FIA_UAU.4.1

Application Note:

The ownership token from the TCPA specification is the 160 bit blob.

5.1.0.30 - User identification before any action (FIA_UID.2)

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user. FIA_UID.2.1

5.1.0.31 - Management of security functions behaviour (FMT_MOF.1)

The TSF shall restrict the ability to disable enable the functions create, delete, load and change owner to owner of entity. FMT_MOF.1.1

5.1.0.32 - Management of security attributes (FMT_MSA.1)

The TSF shall enforce the TCPA ownership protocol for TPM owner or entity owner to restrict the ability to change_default query modify deletenone the security attributes **migration**, location to TPM owner, entity owner. FMT_MSA.1.1

5.1.0.33 - Secure security attributes (FMT_MSA.2)

The TSF shall ensure that only secure values are accepted for security attributes. FMT_MSA.2.1

5.1.0.34 - Static attribute initialisation (FMT_MSA.3)

The TSF shall enforce the TCPA flow control to provide restrictive default values for security attributes that are used to enforce the SFP. FMT_MSA.3.1

The TSF shall allow the TPM owner, entity owner to specify alternative initial values to override the default values when an object or information is created. FMT_MSA.3.2

5.1.0.35 - Management of TSF data (FMT_MTD.1)

The TSF shall restrict the ability to change_default query modify delete clearmigration, backup the all shielded locations to owner. FMT_MTD.1.1

5.1.0.36 - Management of limits on TSF data (FMT_MTD.2)

The TSF shall restrict the specification of the limits for endorsement **key**, SRK, identities to TPM owner. FMT_MTD.2.1

The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: not allow additional entities. FMT_MTD.2.2

5.1.0.37 - Secure TSF data (FMT_MTD.3)

The TSF shall ensure that only secure values are accepted for TSF data. FMT_MTD.3.1

5.1.0.38 - Revocation (FMT_REV.1)

The TSF shall restrict the ability to revoke security attributes associated with the objects other additional resources within the TSC to TPM owner. FMT_REV.1.1

The TSF shall enforce the rules TPM owner only. FMT_REV.1.2

5.1.0.39 - Restrictions on security roles (FMT_SMR.2)

The TSF shall maintain the roles: TPM owner, entity owner. FMT_SMR.2.1

The TSF shall be able to associate users with roles. FMT_SMR.2.2

The TSF shall ensure that the conditions presentation of ownership token proves role are satisfied. FMT_SMR.2.3

satisfied. FMT_SMR.2.3

5.1.0.40 - Anonymity without soliciting information (FPR_ANO.2)

The TSF shall ensure that challengers unable to associate identity with endorsement keyaudit events, identity creation. FPR_ANO.2.1
The TSF shall provide RNG, protected storage to TPM users without soliciting any reference to the real user name. FPR_ANO.2.2

5.1.0.41 - Unlinkability (FPR_UNL.1)

The TSF shall ensure that TPM owner, entity owners are unable to determine whether create identity were caused by the same useridentity to identity. FPR_UNL.1.1

5.1.0.42 - Abstract machine testing (FPT_AMT.1)

The TSF shall run a suite of tests during initial start-up periodically during normal operation at the request of an authorised user to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF. FPT

5.1.0.43 - Failure with preservation of secure state (FPT_FLS.1)

The TSF shall preserve a secure state when the following types of failures occur: bad RNG values, RSA encrypt **decrypt** failure, SHA failure, PCR failure. FPT_FLS.1.1

5.1.0.44 - Inter-TSF detection of modification (FPT_ITI.1)

The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: messages use HMAC to determine that message is intact. FPT_ITI.1.1
The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform ignore command if modifications are detected. FPT_ITI.1.2

5.1.0.45 - TSF data transfer separation (FPT_ITT.2)

The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE. FPT_ITT.2.1
The TSF shall separate user data from TSF data when such data is transmitted between separate parts of the TOE. FPT_ITT.2.2

5.1.0.46 - Passive detection of physical attack (FPT_PHP.1)

The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF. FPT_PHP.1.1
The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred. FPT_PHP.1.2

5.1.0.47 - Resistance to physical attack (FPT_PHP.3)

The TSF shall resist removal from platform to the TPM module and the shielded locations by responding automatically such that the TSP is not violated. FPT_PHP.3.1

5.1.0.48 - Physical Emanations Security (FPT_PHP_EMSEC_Design)

Process emanation FPT_PHP_EMSEC_D.1

Connection emanation FPT_PHP_EMSEC_D.2

5.1.0.49 - Automated recovery without undue loss (FPT_RCV.3)

When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided. FPT_RCV.3.1
For RNG failing self-test, the TSF shall ensure the return of the TOE to a secure state using automated procedures. FPT_RCV.3.2
The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding SRK - and all protected storage underneath the SRK for loss of TSF data or objects within the TSC. FPT_R
The TSF shall provide the capability to determine the objects that were or were not capable of being recovered. FPT_RCV.3.4

5.1.0.50 - Function recovery (FPT_RCV.4)

The TSF shall ensure that Protected storage - loss of info, identities - loss of protected storage, RNG - randomness failure, loss of endorsement have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state. FPT_RCV.4.1

5.1.0.51 - Replay detection (FPT_RPL.1)

The TSF shall detect replay for the following entities: authorization requests. FPT_RP
The TSF shall perform generate audit event, destroy session, disable TPM?????? when replay is detected. FPT_RPL.1.2

5.1.0.52 - SFP domain separation (FPT_SEP.2)

The unisolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. FPT_SEP.2.1
The TSF shall enforce separation between the security domains of subjects in the TSC. FPT_SEP.2.2
The TSF shall maintain the part of the TSF related to TCPA ownership protocol and TCPA flow control in a security domain for their own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to those SFPs. FPT_SEP.2.3

5.1.0.53 - Mutual trusted acknowledgement (FPT_SSP.2)

The TSF shall acknowledge, when requested by another part of the TSF, the receipt of an unmodified TSF data transmission. FPT_SSP.2.1
The TSF shall ensure that the relevant parts of the TSF know the correct status of transmitted data among its different parts, using acknowledgements. FPT_SSP.2.2

5.1.0.54 - Inter-TSF basic TSF data consistency (FPT_TDC.1)

The TSF shall provide the capability to consistently interpret Endorsement **key**, SRK when shared between the TSF and another trusted IT product. FPT_TDC.1.1
The TSF shall use distinguish between endorsement **key** and SRK when interpreting the TSF data from another trusted IT product. FPT_TDC.1.2

5.1.0.55 - Internal TSF consistency (FPT_TRC.1)

The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE. FPT_TRC.1.1

When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for use of endorsement **key**, use of SRK. FPT_TRC.1.2

5.1.0.56 - TSF testing (FPT_TST.1)

The TSF shall run a suite of self tests during initial start-up periodically during normal operation at the request of the authorised user at the conditionsRNG runs tests to ensure that the RNG is not in a stuck state to demonstrate the correct operation of the TSF. FPT_TST.1.1

The TSF shall provide authorised users with the capability to verify the integrity of TSF data. FPT_TST.1.2

The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code. FPT_TST.1.3

5.1.0.57 - Degraded fault tolerance (FRU_FLT.1)

The TSF shall ensure the operation of RSA encrypt, RSA **decrypt**, RNG, RSA **key** generation, entity attribute enforcement when the following failures occur: RSA algorithm failure, RNG failure . FRU_FLT.1.1

5.1.0.58 - Limited priority of service (FRU_PRS.1)

The TSF shall assign a priority to each subject in the TSF. FRU_PRS.1.1

The TSF shall ensure that each access to entities and ownership protocol shall be mediated on the basis of the subjects assigned priority. FRU_PRS.1.2

5.1.0.59 - Basic limitation on multiple concurrent sessions (FTA_MCS.1)

The TSF shall restrict the maximum number of concurrent sessions that belong to the

The TSF shall restrict the maximum number of concurrent sessions that belong to the same user. FTA_MCS.1.1

The TSF shall enforce, by default, a limit of 2 sessions per user. FTA_MCS.1.2

5.1.0.60 - Inter-TSF trusted channel (FTP_ITC.1)

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and **protection** of the channel data from modification or disclosure. FTP_ITC.1.1

The TSF shall permit the remote trusted IT product to initiate communication via the trusted channel. FTP_ITC.1.2

The TSF shall initiate communication via the trusted channel for assignment of ownership token. FTP_ITC.1.3

5.1.0.61 - Trusted path (FTP_TRP.1)

The TSF shall provide a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and **protection** of the communicated data from modification or disclosure. FTP_TRP.1.1

The TSF shall permit remote users to initiate communication via the trusted path. FTP_TRP.1.2

The TSF shall require the use of the trusted path for initial user authentication all protected functions. FTP_TRP.1.3

5.2 - TOE Security Assurance Requirements

Table 5-1 Assurance Requirements: EAL(3)

Assurance Class	Assurance Components

ACM	ACM_CAP.3 ACM_SCP.1
ADO	ADO_DEL.1 ADO_IGS.1
ADV	ADV_FSP.1 ADV_HLD.2 ADV_RCR.1 ADV_SPM.1
AGD	AGD_ADM.1 AGD_USR.1
ALC	ALC_DVS.1 ALC_LCD.1
ATE	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_MSU.1 AVA_SOF.1 AVA_VLA.1

5.2.1 - Configuration management (ACM)

5.2.1.1 - Authorisation controls (ACM_CAP.3)

The CM system shall provide measures such that only authorised changes are made to the configuration items. ACM_CAP.3.10C

The reference for the TOE shall be unique to each version of the TOE. ACM_CAP.3.1C

The developer shall provide a reference for the TOE. ACM_CAP.3.1D

The TOE shall be labelled with its reference. ACM_CAP.3.2C

The developer shall use a CM system. ACM_CAP.3.2D

The CM documentation shall include a configuration list and a CM plan. ACM_CAP.3.3C

The developer shall provide CM documentation. ACM_CAP.3.3D

The configuration list shall describe the configuration items that comprise the TOE. ACM_CAP.3.4C

The CM documentation shall describe the method used to uniquely identify the configuration items. ACM_CAP.3.5C

The CM system shall uniquely identify all configuration items. ACM_CAP.3.6C

The CM plan shall describe how the CM system is used. ACM_CAP.3.7C

The evidence shall demonstrate that the CM system is operating in accordance with the CM plan. ACM_CAP.3.8C

The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system. ACM_CAP.3.9C

5.2.1.2 - TOE CM coverage (ACM_SCP.1)

The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation. ACM_SCP.1.1C

The developer shall provide CM documentation. ACM_SCP.1.1D

The CM documentation shall describe how configuration items are tracked by the CM system. ACM_SCP.1.2C

5.2.2 - Delivery and operation (ADO)

5.2.2.1 - Delivery procedures (ADO_DEL.1)

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site. ADO_DEL.1.1C

The developer shall document procedures for delivery of the TOE or parts of it to the user. ADO_DEL.1.1D

The developer shall use the delivery procedures. ADO_DEL.1.2D

5.2.2.2 - Installation, generation, and start-up procedures (ADO_IGS.1)

The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE. ADO_IGS.1.1C

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE. ADO_IGS.1.1D

5.2.3 - Development (ADV)

5.2.3.1 - Informal functional specification (ADV_FSP.1)

The functional specification shall describe the TSF and its external interfaces using an informal style. ADV_FSP.1.1C

The developer shall provide a functional specification. ADV_FSP.1.1D

The functional specification shall be internally consistent. ADV_FSP.1.2C

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate. ADV_FSP.1.3C

The functional specification shall completely represent the TSF. ADV_FSP.1.4C

5.2.3.2 - Security enforcing high-level design (ADV_HLD.2)

The presentation of the high-level design shall be informal. ADV_HLD.2.1C

The developer shall provide the high-level design of the TSF. ADV_HLD.2.1D

The high-level design shall be internally consistent. ADV_HLD.2.2C

The high-level design shall describe the structure of the TSF in terms of

subsystems. ADV_HLD.2.3C

The high-level design shall describe the security functionality provided by each subsystem of the TSF. ADV_HLD.2.4C

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting **protection** mechanisms implemented in that hardware, firmware, or software. ADV_

The high-level design shall identify all interfaces to the subsystems of the TSF. ADV_HLD.2.6C

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible. ADV_HLD.2.7C

The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate. ADV_HLD.2.8C

The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems. ADV_HLD.2.9C

5.2.3.3 - Informal correspondence demonstration (ADV_RCR.1)

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation. ADV_RCR.1.1C

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided. ADV_RCR.1.1D

5.2.3.4 - Informal TOE security policy model (ADV_SPM.1)

The TSP model shall be informal. ADV_SPM.1.1C

The TSP model shall be informal.

The developer shall provide a TSP model. ADV_SPM.1.1D

The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled. ADV_SPM.1.2C

The developer shall demonstrate correspondence between the functional specification and the TSP model. ADV_SPM.1.2D

The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled. ADV_SPM.1.3C

The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model. ADV_SPM.1.4C

Application Note:

The inclusion of the security policy allows the correlation of the **protection** profile to the specification to have a complete description. The policy allows for a single spot to include the access control and execution policies that the specification requires. This document allows the developer to better understand the reasoning and requirements that the specification and profile require.

5.2.4 - Guidance documents (AGD)

5.2.4.1 - Administrator guidance (AGD_ADM.1)

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE. AGD_ADM.1.1C

The developer shall provide administrator guidance addressed to system administrative personnel. AGD_ADM.1.1D

The administrator guidance shall describe how to administer the TOE in a secure manner. AGD_ADM.1.2C

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment. AGD_ADM.1.3C

The administrator guidance shall describe all assumptions regarding user behaviour that

are relevant to secure operation of the TOE. AGD_ADM.1.4C

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate. AGD_ADM.1.5C

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF. AGD_ADM.1.6C

The administrator guidance shall be consistent with all other documentation supplied for evaluation. AGD_ADM.1.7C

The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator. AGD_ADM.1.8C

5.2.4.2 - User guidance (AGD_USR.1)

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE. AGD_USR.1.1C

The developer shall provide user guidance. AGD_USR.1.1D

The user guidance shall describe the use of user-accessible security functions provided by the TOE. AGD_USR.1.2C

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment. AGD_USR.1.3C

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment. AGD_USR.1.4C

The user guidance shall be consistent with all other documentation supplied for evaluation. AGD_USR.1.5C

The user guidance shall describe all security requirements for the IT environment that are relevant to the user. AGD_USR.1.6C

5.2.5 - Life cycle support (ALC)

5.2.5.1 - Identification of security measures (ALC_DVS.1)

The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. ALC_DVS.1.1C

The developer shall produce development security documentation. ALC_DVS.1.1D

The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE. ALC_D

5.2.5.2 - Developer defined life-cycle model (ALC_LCD.1)

The life-cycle definition documentation shall describe the model used to develop and maintain the TOE. ALC_LCD.1.1C

The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE. ALC_LCD.1.1D

The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE. ALC_LCD.1.2C

The developer shall provide life-cycle definition documentation. ALC_LCD.1.2D

5.2.6 - Tests (ATE)

5.2.6.1 - Analysis of coverage (ATE_COV.2)

The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. ATE_COV.2.1C

The developer shall provide an analysis of the test coverage. ATE_COV.2.1D

The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete. ATE_COV.2.2C

5.2.6.2 - Testing: high-level design (ATE_DPT.1)

The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design. ATE_DPT.1.1C

The developer shall provide the analysis of the depth of testing. ATE_DPT.1.1D

5.2.6.3 - Functional testing (ATE_FUN.1)

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results. ATE_FUN.1.1C

The developer shall test the TSF and document the results. ATE_FUN.1.1D

The test plans shall identify the security functions to be tested and describe the goal of the ATE_FUN.1.2C

tests to be performed. ATE_FUN.1.2C

The developer shall provide test documentation. ATE_FUN.1.2D

The test procedure descriptions shall identify the tests to be performed and describe the

scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests. ATE_FUN.1.3C

The expected test results shall show the anticipated outputs from a successful execution of the tests. ATE_FUN.1.4C

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified. ATE_FUN.1.5C

5.2.6.4 - Independent testing - sample (ATE_IND.2)

The TOE shall be suitable for testing. ATE_IND.2.1C

The developer shall provide the TOE for testing. ATE_IND.2.1D

The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF. ATE_IND.2.2C

5.2.7 - Vulnerability assessment (AVA)

5.2.7.1 - Examination of guidance (AVA_MSU.1)

The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation. AVA_MSU.1.1C

The developer shall provide guidance documentation. AVA_MSU.1.1D

The guidance documentation shall be complete, clear, consistent and reasonable. AVA_MSU.1.2C

The guidance documentation shall list all assumptions about the intended environment. AVA_MSU.1.3C

The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls). AVA_MSU.1.4C

5.2.7.2 - Strength of TOE security function evaluation (AVA_SOF.1)

5.2.7.2 - Strength of TOE security function evaluation (AVA_SOF.1)

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST. AVA_SOF.1.1C

The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim. AVA_SOF.1.1D

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST. AVA_SOF.1.2C

5.2.7.3 - Developer vulnerability analysis (AVA_VLA.1)

The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. AVA_VLA.1.1C

The developer shall perform and document an analysis of the TOE deliverables searching

for obvious ways in which a user can violate the TSP. AVA_VLA.1.1D

The developer shall document the disposition of obvious vulnerabilities. AVA_VLA.1.2D

5.3 - Security Requirements for the IT Environment (Optional)

5.3.0.1 - Potential violation analysis (FAU_SAA.1)

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP. FAU_SAA.1.1

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of authorization failure passing a threshold value known to indicate a potential security violation;

FAU_SAA.1.2

b) RNG failure. FAU_SAA.1.2

Application Note:

The TPS can monitor the audit log and issue commands to the TPM cause it to cease providing information. The mechanism can be as simple as writing new values to all PCR registers causing all LOADS using PCR registers to fail.

5.3.0.2 - Audit review (FAU_SAR.1)

The TSF shall provide authorised users with the capability to read all audit records from the audit records. FAU_SAR.1.1

The TSF shall provide the audit records in a manner suitable for the user to interpret the information. FAU_SAR.1.2

Application Note:

The TPM provides the audit event in a manner that only the TPS can access. This requires that the TPS block access to the audit event port.

5.3.0.3 - Protected audit trail storage (FAU_STG.1)

The TSF shall protect the stored audit records from unauthorised deletion. FAU_STG.

The TSF shall be able to detect modifications to the audit records. FAU_STG.1.2

Application Note:

The audit log is kept by the TPS, however the TPM keeps the mechanism that allows for detection of audit log tampering. This mechanism is the keeping of each audit log event in a PCR like register and then hashing in each subsequent audit event. The log, when

tampered with, will not be able to recreate the same value that is in the audit register and hence the challenger will know of audit log tampering. The challenger may not be able to recreate the damage to the log.

recreate the damage to the log.

5.4 - Security Requirements for the Non-IT Environment (Optional)

Identify the IT security requirements that are to be met by the IT environment of the TOE. If the TOE has no asserted dependencies on the IT environment, this section may be omitted.

The trusted path is the establishment of the ephemeral session from the TCPA specification. This session establishes that both endpoints are known (i.e. they both have knowledge of the authentication token) and each subsequent communication requires the proving of knowledge of the ephemeral session **key**.

6 - Rationale

Include an overall summary of rationale.

6.1 - Introduction and TOE Description Rationale (Optional)

Presents the rationale used in the **protection** profile evaluation.

6.2 - Security Objectives Rationale

Table 6-1 Mapping the TOE Security Environment to Security Objectives

Policy/Threat/Assumptions	**Objectives**
	Security Objectives for the TOE
A.Application_use	O.Protected_Capability
A.Configuration	O.NoBore, O.Admin_Guidance, O.User_Guidance
A.Conformance	O.SpecRef

TCPA Security Policy

A.Hostile_User	O.NoBore
A.Outsider_Med	O.NoBore
A.Physical	O.Protected_Capability
A.System	O.SpecRef
A.TCPAIdentityCertification	O.TCPAProtectedStorage, O.TCPAIdentities
A.TCPARootMeasurement	O.SpecRef
A.Trusted_User	O.User_Defined_AC
P.Accountability	O.Audit_Generation, O.User_Defined_AC
P.Authorities	O.Admin_Guidance
P.Availability	O.Config_Management, O.Sys_Backup_Procs, O.Sys_Backup_Verify
P.EMI_EMC	O.EMSEC_Design
P.Guidance	O.Admin_Guidance, O.User_Guidance
P.Information_AC	O.TCPAProtectedStorage
P.Integrity	O.Security_Attr_Mgt, O.Security_Data_Mgt, O.Security_Func_Mgt, O.Change_Control_Users, O.Trusted_Recovery_Doc, O.Integrity_Data/SW, O.Integrity_Practice, O.Malicious_Code, O.Storage_Integrity, O.Sys_Assur_HW/SW/FW, O.Config_Management, O.Sys_Self_Protection, O.User_Data_Integrity, O.User_Defined_AC,

	O.User_Data_Integrity, O.User_Defined_AC, O.User_Data_Transfer
P.Lifecycle	O.Lifecycle_Security
P.Marking	O.External_Labels
P.MessageAuth	O.SpecRef, O.MessageAuthentication
P.Physical_Control	O.Tamper_ID
P.SpecRef	O.SpecRef, O.AuditLog, O.RootMeasurement, O.RootReporting, O.SecureManufacturing

---

TCPA Security Policy

P.TCPAAuthorization	O.SpecRef, O.MetricReporting, O.TCPAProtectedStorage
P.TCPAIdentities	O.TCPAIdentities, O.TCPAProtectedStorage
P.TCPAOwnership	O.SpecRef, O.TCPAProtectedStorage
P.TCPAProtectMigrate	O.TCPAProtectedStorage
P.TCPARegDIR	O.SpecRef, O.TCPAProtectedStorage
P.TCPARegPCR	O.SpecRef, O.MetricReporting, O.TCPAProtectedStorage
P.TSP	O.SpecRef, Security Objectives
T.Admin_Err_Commit	O.Admin_Guidance, O.Crypto_Key_Man, O.Security_Attr_Mgt, O.Security_Data_Mgt, O.Security_Func_Mgt, O.Security_Roles, O.Limit_Actions_Auth

	O.Limit_Actions_Auth
T.Admin_Err_Omit	O.Admin_Guidance, O.Crypto_Key_Man, O.User_Auth_Management
T.Admin_UserPriv	O.Prevent_Link
T.Component_Failure	O.Crypto_Key_Man, O.Crypto_Data_Sep, O.Crypto_Dsgn_Impl, O.Crypto_Modular_Dsgn, O.Crypto_Operation, O.Crypto_Self_Test, O.Crypto_Test_Reqs, O.Fail_Secure, O.Fault_Tolerance, O.Secure_State
T.Dev_Flawed_Code	O.Code_Signing, O.Integ_Sys_Data_Int, O.No_Residual_Info, O.Secure_State, O.Sys_Self_Protection, O.Integ_Sys_Data_Ext, O.Source_Code_Exam
T.EndorseExpose	O.NoBore, O.Protected_Capability, O.SpecRef, O.TCPAIdentities, O.RootReporting, O.Admin_Guidance, O.Code_Signing, O.Crypto_Data_Sep, O.Crypto_Dsgn_Impl, O.Crypto_Key_Man, O.Fault_Tolerance, O.Fail_Secure, O.Integ_Sys_Data_Ext, O.Integ_Sys_Data_Int, O.MetricReporting, O.EMSEC_Design, O.Trusted_Recovery_Doc, O.Trusted_Recovery

T.Failure_DS_Comp	O.Fault_Tolerance, O.Integrity_Data_Rep
T.GlobalSecret	O.NoBore, O.Crypto_Dsgn_Impl
T.Hack_AC	O.Trusted_Path, O.Apply_Code_Fixes, O.AuditLog

T.Hack_Avl_Resource	O.Audit_Generation, O.Hack_Limit_Sessions, O.Manage_TSF_Data, O.React_Discovered_Atk, O.Data_Imp_Exp_Control, O.AuditLog
T.Hack_Comm_Eavesdrop	O.Data_Exchange_Conf
T.Hack_Crypto	O.Crypto_Data_Sep, O.EMSEC_Design, O.IntelEman_Control, O.IntelEman_Contain, O.SpecRef, O.Protected_Capability
T.Hack_Msg_Data	O.Rcv_MsgMod_ID, O.Snt_MsgMod_ID, O.TSF_Rcv_Err_ID_Loc, O.TSF_Rcv_Err_ID_Rem, O.TSF_Snd_Err_ID_Loc, O.TSF_Snd_Err_ID_Rem, O.AuditLog
T.Hack_Phys	O.EMSEC_Design, O.Tamper_ID, O.Tamper_Resistance, O.IntelEman_Contain, O.IntelEman_Control
T.Hack_Social_Engineer	O.Admin_Guidance, O.User_Guidance
T.IdenClone	O.TCPAIdentities, O.RootReporting, O.Crypto_Data_Sep, O.Export_Control, O.External_Labels, O.Integ_User_Data_Int, O.MetricReporting
T.IdenPKI	O.TCPAIdentities, O.RootReporting, O.MetricReporting
T.Malicious_Code	O.Trusted_Path, O.Admin_Code_Val, O.Clean_Obj_Recovery, O.Code_Signing, O.General_Integ_Checks, O.Obj_Protection, O.Input_Inspection, O.AuditLog
T.MeasureFalse	O.RootMeasurement
T.OwnerMasquerade	O.SpecRef, O.TCPAIdentities, O.TCPAProtectedStorage, O.Crypto_Data_Sep, O.Crypto_Dsgn_Impl, O.User_Auth_Management, O.User_Conf_Prevention
T.Power_Disrupt	O.Atomic_Functions, O.Trusted_Recovery

T.ProtStorAttribute	O.Protected_Capability, O.TCPAProtectedStorage, O.Crypto_Data_Sep, O.Data_Exchange_Conf, O.External_Labels, O.Integ_Data_Mark_Exp, O.Integ_User_Data_Int, O.Integrity_Data/SW, O.User_Data_Integrity
T.ProtStoreBackup	O.TCPAProtectedStorage, O.TCPAIdentities, O.Crypto_Dsgn_Impl, O.Export_Control, O.External_Labels, O.Integ_Data_Mark_Exp, O.Trusted_Recovery_Doc, O.Trusted_Recovery
T.ProtStoreCrypto	O.Protected_Capability, O.TCPAProtectedStorage, O.Crypto_Data_Sep, O.Crypto_Dsgn_Impl, O.User_Data_Integrity
T.ProtStoreMaintenance	O.TCPAProtectedStorage, O.Protected_Capability, O.TCPAIdentities, O.Crypto_Dsgn_Impl, O.Data_Exchange_Conf, O.Export_Control, O.External_Labels, O.Integ_Data_Mark_Exp, O.Trusted_Recovery_Doc, O.Trusted_Recovery
T.Repudiate_Receive	O.NonRepud_Assess_Recd, O.NonRepud_Gen_Recd
T.Repudiate_Send	O.NonRepud_Assess_Sent, O.NonRepud_Gen_Sent
T.Repudiate_Transact	O.NonRepud_Assess_Recd, O.NonRepud_Assess_Sent, O.NonRepud_Gen_Recd, O.NonRepud_Gen_Sent
T.SpecRef	O.SpecRef, O.Integrity_Data/SW, O.AuditLog, O.MetricReporting, O.Fail_Secure, O.Fault_Tolerance, O.General_Integ_Checks, O.Integ_Data_Mark_Exp, O.Integ_Sys_Data_Ext, O.Integ_Sys_Data_Int, O.Integ_User_Data_Int, O.Integrity_Data_Rep, O.Lifecycle_Security, O.Integrity_Practice, O.Limit_Actions_Auth, O.Maintain_Sec_Domain, O.Malicious_Code, O.Manage_Res_Sec_Attr,

	O.Manage_TSF_Data, O.No_Residual_Info
T.Spoofing	O.Trusted_Path
T.User_Abuse_Conf	O.Admin_Code_Val, O.Admin_Guidance, O.Data_Export_Control, O.Export_Control, O.Standard_Output_Pres, O.AuditLog, O.SpecRef
T.User_Collect	O.Audit_Generation, O.Trusted_Path, O.User_Defined_AC, O.Data_Exchange_Conf,

	O.Info_Flow_Control, O.Integ_User_Data_Int, O.No_Residual_Info, O.Security_Roles
T.User_Err_Conf	O.AC_Label_Export, O.Crypto_AC, O.Crypto_Import_Export, O.Crypto_Key_Man, O.User_Conf_Prevention, O.SpecRef, O.TCPAIdentities
T.User_Err_Inaccess	O.User_Guidance, O.Security_Attr_Mgt
T.User_Err_Integrity	O.AC_Label_Export, O.Audit_Generation, O.Crypto_Import_Export, O.Info_Flow_Control, O.User_Defined_AC, O.SpecRef
T.User_Err_Slf_Protect	O.AC_Label_Export, O.Obj_Attr_Integrity
T.User_Misuse_Avl_Resc	O.Audit_Generation, O.Manage_TSF_Data, O.Tamper_ID, O.Data_Imp_Exp_Control, O.Limit_Comm_Sessions, O.Manage_Res_Sec_Attr, O.Tamper_Resistance, O.SpecRef
	O.Audit_Generation, O.Config_Management, O.General_Integ_Checks, O.Info_Flow_Control, O.Integrity_Practice, O.Security_Data_Mgt,

T.User_Modify	O.Integrity_Practice, O.Security_Data_Mgt, O.Security_Roles, O.User_Defined_AC, O.Integ_Sys_Data_Int, O.Maintain_Sec_Domain, O.SpecRef
T.User_Send	O.Admin_Code_Val, O.Audit_Generation, O.Export_Control, O.Standard_Output_Pres, O.Integ_Data_Mark_Exp, O.SpecRef

Security Objectives for the Environment

P.SpecRef	O.AuditLog
T.Admin_Err_Commit	O.Audit_Protect
T.Hack_AC	O.Trusted_Path, O.AuditLog
T.Hack_Avl_Resource	O.AuditLog
T.Hack_Msg_Data	O.AuditLog
T.Malicious_Code	O.Trusted_Path, O.AuditLog
T.SpecRef	O.AuditLog

T.Spoofing	O.Trusted_Path
T.User_Abuse_Conf	O.AuditLog
T.User_Collect	O.Trusted_Path
T.User_Modify	O.Audit_Protect

Table 6-2 Tracing of Security Objectives to the TOE Security Environment

Objectives	Policy/Threat/Assumptions
	Security Objectives for the TOE
O.AC_Label_Export	T.User_Err_Conf, T.User_Err_Integrity, T.User_Err_Slf_Protect
O.Admin_Code_Val	T.Malicious_Code, T.User_Abuse_Conf, T.User_Send
O.Admin_Guidance	A.Configuration, P.Authorities, P.Guidance, T.Admin_Err_Commit, T.Admin_Err_Omit, T.EndorseExpose, T.Hack_Social_Engineer, T.User_Abuse_Conf
O.Apply_Code_Fixes	T.Hack_AC
O.Atomic_Functions	T.Power_Disrupt
O.AuditLog	P.SpecRef, T.Hack_AC, T.Hack_Avl_Resource, T.Hack_Msg_Data, T.Malicious_Code, T.SpecRef, T.User_Abuse_Conf
O.Audit_Generation	P.Accountability, T.Hack_Avl_Resource, T.User_Collect, T.User_Err_Integrity, T.User_Misuse_Avl_Resc, T.User_Modify, T.User_Send
O.Change_Control_Users	P.Integrity
O.Clean_Obj_Recovery	T.Malicious_Code
O.Code_Signing	T.Dev_Flawed_Code, T.EndorseExpose, T.Malicious_Code
O.Config_Management	P.Availability, P.Integrity, T.User_Modify

O.Crypto_AC	T.User_Err_Conf
O.Crypto_Data_Sep	T.Component_Failure, T.EndorseExpose, T.Hack_Crypto, T.IdenClone, T.OwnerMasquerade, T.ProtStorAttribute, T.ProtStoreCrypto
O.Crypto_Dsgn_Impl	T.Component_Failure, T.EndorseExpose, T.GlobalSecret, T.OwnerMasquerade, T.ProtStoreBackup, T.ProtStoreCrypto, T.ProtStoreMaintenance
O.Crypto_Import_Export	T.User_Err_Conf, T.User_Err_Integrity
O.Crypto_Key_Man	T.Admin_Err_Commit, T.Admin_Err_Omit, T.Component_Failure, T.EndorseExpose, T.User_Err_Conf
O.Crypto_Modular_Dsgn	T.Component_Failure
O.Crypto_Operation	T.Component_Failure
O.Crypto_Self_Test	T.Component_Failure
O.Crypto_Test_Reqs	T.Component_Failure
O.Data_Exchange_Conf	T.Hack_Comm_Eavesdrop, T.ProtStorAttribute, T.ProtStoreMaintenance, T.User_Collect
O.Data_Export_Control	T.User_Abuse_Conf
O.Data_Imp_Exp_Control	T.Hack_Avl_Resource, T.User_Misuse_Avl_Resc
O.EMSEC_Design	P.EMI_EMC, T.EndorseExpose, T.Hack_Crypto, T.Hack_Phys
O.Export_Control	T.IdenClone, T.ProtStoreBackup, T.ProtStoreMaintenance, T.User_Abuse_Conf, T.User_Send
O.External_Labels	P.Marking, T.IdenClone, T.ProtStorAttribute, T.ProtStoreBackup, T.ProtStoreMaintenance

O.Fail_Secure	T.Component_Failure, T.EndorseExpose, T.SpecRef
O.Fault_Tolerance	T.Component_Failure, T.EndorseExpose, T.Failure_DS_Comp, T.SpecRef
O.General_Integ_Checks	T.Malicious_Code, T.SpecRef, T.User_Modify

O.Hack_Limit_Sessions	T.Hack_Avl_Resource
O.Info_Flow_Control	T.User_Collect, T.User_Err_Integrity, T.User_Modify
O.Input_Inspection	T.Malicious_Code
O.Integ_Data_Mark_Exp	T.ProtStorAttribute, T.ProtStoreBackup, T.ProtStoreMaintenance, T.SpecRef, T.User_Send
O.Integ_Sys_Data_Ext	T.Dev_Flawed_Code, T.EndorseExpose, T.SpecRef
O.Integ_Sys_Data_Int	T.Dev_Flawed_Code, T.EndorseExpose, T.SpecRef, T.User_Modify
O.Integ_User_Data_Int	T.IdenClone, T.ProtStorAttribute, T.SpecRef, T.User_Collect
O.Integrity_Data/SW	P.Integrity, T.ProtStorAttribute, T.SpecRef
O.Integrity_Data_Rep	T.Failure_DS_Comp, T.SpecRef
O.Integrity_Practice	P.Integrity, T.SpecRef, T.User_Modify
O.IntelEman_Contain	T.Hack_Crypto, T.Hack_Phys
O.IntelEman_Control	T.Hack_Crypto, T.Hack_Phys

O.Lifecycle_Security	P.Lifecycle, T.SpecRef
O.Limit_Actions_Auth	T.Admin_Err_Commit, T.SpecRef
O.Limit_Comm_Sessions	T.User_Misuse_Avl_Resc
O.Maintain_Sec_Domain	T.SpecRef, T.User_Modify
O.Malicious_Code	P.Integrity, T.SpecRef
O.Manage_Res_Sec_Attr	T.SpecRef, T.User_Misuse_Avl_Resc
O.Manage_TSF_Data	T.Hack_Avl_Resource, T.SpecRef, T.User_Misuse_Avl_Resc
O.MessageAuthentication	P.MessageAuth
O.MetricReporting	P.TCPAAuthorization, P.TCPARegPCR, T.EndorseExpose, T.IdenClone, T.IdenPKI, T.SpecRef

O.NoBore	A.Configuration, A.Hostile_User, A.Outsider_Med, T.EndorseExpose, T.GlobalSecret
O.No_Residual_Info	T.Dev_Flawed_Code, T.SpecRef, T.User_Collect
O.NonRepud_Assess_Recd	T.Repudiate_Receive, T.Repudiate_Transact
O.NonRepud_Assess_Sent	T.Repudiate_Send, T.Repudiate_Transact
O.NonRepud_Gen_Recd	T.Repudiate_Receive, T.Repudiate_Transact
O.NonRepud_Gen_Sent	T.Repudiate_Send, T.Repudiate_Transact

O.Obj_Attr_Integrity	T.User_Err_Slf_Protect
O.Obj_Protection	T.Malicious_Code
O.Prevent_Link	T.Admin_UserPriv
O.Protected_Capability	A.Application_use, A.Physical, T.EndorseExpose, T.Hack_Crypto, T.ProtStorAttribute, T.ProtStoreCrypto, T.ProtStoreMaintenance
O.Rcv_MsgMod_ID	T.Hack_Msg_Data
O.React_Discovered_Atk	T.Hack_Avl_Resource
O.RootMeasurement	P.SpecRef, T.MeasureFalse
O.RootReporting	P.SpecRef, T.EndorseExpose, T.IdenClone, T.IdenPKI
O.SecureManufacturing	P.SpecRef
O.Secure_State	T.Component_Failure, T.Dev_Flawed_Code
O.Security_Attr_Mgt	P.Integrity, T.Admin_Err_Commit, T.User_Err_Inaccess
O.Security_Data_Mgt	P.Integrity, T.Admin_Err_Commit, T.User_Modify
O.Security_Func_Mgt	P.Integrity, T.Admin_Err_Commit
O.Security_Roles	T.Admin_Err_Commit, T.User_Collect, T.User_Modify
O.Snt_MsgMod_ID	T.Hack_Msg_Data
O.Source_Code_Exam	T.Dev_Flawed_Code

O.SpecRef	A.Conformance, A.System, A.TCPARootMeasurement, P.MessageAuth, P.SpecRef, P.TCPAAuthorization, P.TCPAOwnership, P.TCPARegDIR, P.TCPARegPCR, P.TSP, T.EndorseExpose, T.Hack_Crypto, T.OwnerMasquerade, T.SpecRef, T.User_Abuse_Conf, T.User_Err_Conf, T.User_Err_Integrity, T.User_Misuse_Avl_Resc, T.User_Modify, T.User_Send
O.Standard_Output_Pres	T.User_Abuse_Conf, T.User_Send
O.Storage_Integrity	P.Integrity
O.Sys_Assur_HW/SW/FW	P.Integrity
O.Sys_Backup_Procs	P.Availability
O.Sys_Backup_Verify	P.Availability
O.Sys_Self_Protection	P.Integrity, T.Dev_Flawed_Code
O.TCPAIdentities	A.TCPAIdentityCertification, P.TCPAIdentities, T.EndorseExpose, T.IdenClone, T.IdenPKI, T.OwnerMasquerade, T.ProtStoreBackup, T.ProtStoreMaintenance, T.User_Err_Conf
O.TCPAProtectedStorage	A.TCPAIdentityCertification, P.Information_AC, P.TCPAAuthorization, P.TCPAIdentities, P.TCPAOwnership, P.TCPAProtectMigrate, P.TCPARegDIR, P.TCPARegPCR, T.OwnerMasquerade, T.ProtStorAttribute, T.ProtStoreBackup, T.ProtStoreCrypto, T.ProtStoreMaintenance
O.TSF_Rcv_Err_ID_Loc	T.Hack_Msg_Data
O.TSF_Rcv_Err_ID_Rem	T.Hack_Msg_Data
O.TSF_Snd_Err_ID_Loc	T.Hack_Msg_Data
O.TSF_Snd_Err_ID_Rem	T.Hack_Msg_Data
O.Tamper_ID	P.Physical_Control, T.Hack_Phys, T.User_Misuse_Avl_Resc

O.Tamper_Resistance	T.Hack_Phys, T.User_Misuse_Avl_Resc
O.Trusted_Path	T.Hack_AC, T.Malicious_Code, T.Spoofing, T.User_Collect

O.Trusted_Recovery	T.EndorseExpose, T.Power_Disrupt, T.ProtStoreBackup, T.ProtStoreMaintenance
O.Trusted_Recovery_Doc	P.Integrity, T.EndorseExpose, T.ProtStoreBackup, T.ProtStoreMaintenance
O.User_Auth_Management	T.Admin_Err_Omit, T.OwnerMasquerade
O.User_Conf_Prevention	T.OwnerMasquerade, T.User_Err_Conf
O.User_Data_Integrity	P.Integrity, T.ProtStorAttribute, T.ProtStoreCrypto
O.User_Data_Transfer	P.Integrity
O.User_Defined_AC	A.Trusted_User, P.Accountability, P.Integrity, T.User_Collect, T.User_Err_Integrity, T.User_Modify
O.User_Guidance	A.Configuration, P.Guidance, T.Hack_Social_Engineer, T.User_Err_Inaccess
Security Objectives	P.TSP

Security Objectives for the Environment

O.AuditLog	P.SpecRef, T.Hack_AC, T.Hack_Avl_Resource, T.Hack_Msg_Data, T.Malicious_Code, T.SpecRef, T.User_Abuse_Conf
O.Audit_Protect	T.Admin_Err_Commit, T.User_Modify

O.Trusted_Path	T.Hack_AC, T.Malicious_Code, T.Spoofing, T.User_Collect

6.2.1 - Policies

P.Accountability: Individual accountability
Individuals shall be held accountable for their actions.

Example detailed policy statements:

- DP.Audit_Generation: Audit data generation with identity
  The system shall provide the capability to ensure that all audit records include enough information to determine the date and time of action, the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved.

This detailed policy statement is addressed by:

1. O.Audit_Generation: Audit records with identity
   Record in audit records: date and time of action, location of the action, and the entity responsible for the action.

- DP.User_Defined_AC: Discretionary access control
  The system shall provide a Discretionary Access Control (DAC) function (i.e., a user can grant access authorization to other users for data they control).
  This detailed policy statement is addressed by:

1. O.User_Defined_AC: User-defined access control
   Enforce an access control policy whereby users may determine who may access information they control.

P.Authorities: Notification of threats and vulnerabilities
Appropriate authorities shall be immediately notified of any threats or vulnerabilities impacting systems that process their data.

In General, P.Authorities is addressed by:

1. O.Admin_Guidance: Administrator guidance documentation
   Deter administrator errors by providing adequate administrator guidance.

P.Availability: Information availability
Information shall be available to satisfy mission requirements.

Example detailed policy statements:

- DP.Config_Mgt_Plan: Implement operational configuration management
  A configuration management plan shall be implemented by the system. The system shall implement configuration management to assure storage integrity, identification of system connectivity (software, hardware, and firmware), and identification of system components (software, hardware, and firmware).
  The system shall implement strong integrity mechanisms (integrity locks, encryption).
  This detailed policy statement is addressed by:

  1. O.Config_Management: Implement operational configuration management
     Implement a configuration management plan. Implement configuration management to assure storage integrity, identification of system connectivity (software, hardware, and firmware), and identification of system components (software, hardware, and firmware).

- DP.Documented_Recovery: Documented recovery
  The system shall provide procedures and features to assure that system recovery is

The system shall provide procedures and features to assure that system recovery is done in a trusted and secure manner. Any circumstances that could result in an untrusted recovery shall be documented.
This detailed policy statement is addressed by:

1. O.Trusted_Recovery_Doc: Documentation of untrusted data recovery
   Provide trusted recovery to ensure that data cannot be lost or misplaced. Any circumstances which can cause untrusted recovery to be documented with mitigating procedures established.

- DP.Malicious_Code: Malicious code prevention
  Procedures and mechanisms to prevent the introduction of malicious code into the system shall be provided.
  This detailed policy statement is addressed by:

  1. O.Malicious_Code: Procedures for preventing malicious code
     Incorporate malicious code prevention procedures and mechanisms.

- DP.Sys_Assur_HW/SW/FW: Validation of security function integrity
  Features and procedures to validate the integrity and the expected operation of the security-relevant software, hardware, and firmware shall be provided by the system.
  This detailed policy statement is addressed by:

  1. O.Sys_Assur_HW/SW/FW: Validation of security function
     Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures.

- DP.Sys_Backup_Procs: System backup procedures
  Provide the capability to restore the system to a secure state after discontinuities of system operations.
  This detailed policy statement is addressed by:

  1. O.Sys_Backup_Procs: System backup procedures
     Provide backup procedures to ensure that the system can be reconstructed.

- DP.Sys_Backup_Verify: Backup **protection** and restoration
  The system shall provide appropriate physical and technical **protection** of the backup and restoration hardware, firmware, and software.
  Safeguard Application: The objective O.Sys_Backup_Verify does not provide

  complete coverage of this policy. Additional objectives need to be defined. Currently detection of failure is accounted for but not prevention of failure.
  This detailed policy statement is addressed by:

1. O.Sys_Backup_Verify: Detect modifications of backup hardware, firmware, software
   Detect modifications to backup hardware, firmware, and software.

- DP.System_Recovery: Trusted system recovery
  Provide procedures and features to assure that system recovery is done in a trusted and secure manner.
  This detailed policy statement is addressed by:

  1. O.Trusted_Recovery_Doc: Documentation of untrusted data recovery
     Provide trusted recovery to ensure that data cannot be lost or misplaced. Any circumstances which can cause untrusted recovery to be documented with mitigating procedures established.

- DP.User_Data_Storage: **Protection** of stored user data
  The system shall provide appropriate storage, continuous personnel access control storage, or encrypted storage of data based on the sensitivity of the data.
  Safeguard Application: O.User_Data_Integrity covers part of this policy, but

  an additional objective dealing with confidentiality may be needed.
  This detailed policy statement is addressed by:

  1. O.User_Data_Integrity: Integrity **protection** of stored user data
     Provide appropriate integrity **protection** for stored user data.

  2. O.User_Defined_AC: User-defined access control
     Enforce an access control policy whereby users may determine who may access information they control.

- DP.User_Data_Transfer: **Protection** of transmitted user data
  The system shall provide a protected distribution system for data transmitted.
  This detailed policy statement is addressed by:

1. O.User_Data_Transfer: **Protection** of transmitted user data
   Provide the ability to have physically protected communications lines, intrusion detection for communications lines, and/or need-to-know isolation for communications lines.

P.EMI_EMC: EMI Emissions
The TOE security policy must specify what level of emissions are permissable when the TOE executes cryptographic operations.

In General, P.EMI_EMC is addressed by:

1. O.EMSEC_Design: Provide physical emanations security
   Design and build the system in such a way as to control the production of intelligible emanations within specified limits.

P.Guidance: Installation and usage guidance
Guidance shall be provided for the secure installation and use of the system.

In General, P.Guidance is addressed by:

1. O.Admin_Guidance: Administrator guidance documentation
   Deter administrator errors by providing adequate administrator guidance.
2. O.User_Guidance: User guidance documentation
   Provide documentation for the general user.

P.Information_AC: Information access control
Information shall be accessed only by authorized individuals and processes.

Example detailed policy statements:

- DP.Admin_Security_Data: Changes to security data by authorized personnel
  Provide mechanisms to assure that changes to security related data are executed

only by authorized personnel.
This detailed policy statement is addressed by:

1. O.Security_Attr_Mgt: Manage security attributes
   Manage the initialization of, values for, and allowable operations on security attributes.

2. O.Security_Data_Mgt: Manage security-critical data
   Manage the initialization of, limits on, and allowable operations on security-critical data.

3. O.Security_Func_Mgt: Manage behavior of security functions
   Provide management mechanisms for security mechanisms.

- DP.User_Defined_AC: Discretionary access control
  The system shall provide a Discretionary Access Control (DAC) function (i.e., a user can grant access authorization to other users for data they control).
  This detailed policy statement is addressed by:

  1. O.User_Defined_AC: User-defined access control
     Enforce an access control policy whereby users may determine who may access information they control.

In General, P.Information_AC is addressed by:

1. O.TCPAProtectedStorage: TCPA Protective Storage
   The TOE must provide a protected storage mechanism as defined in the specification section 3.6 and chapter 6.

P.Integrity: Information content integrity
Information shall retain its content integrity.

Example detailed policy statements:

- DP.Admin_Security_Data: Changes to security data by authorized personnel
  Provide mechanisms to assure that changes to security related data are executed only by authorized personnel.
  This detailed policy statement is addressed by:

  1. O.Security_Attr_Mgt: Manage security attributes
     Manage the initialization of, values for, and allowable operations on security attributes.

  2. O.Security_Data_Mgt: Manage security-critical data
     Manage the initialization of, limits on, and allowable operations on security-critical data.

  3. O.Security_Func_Mgt: Manage behavior of security functions
     Provide management mechanisms for security mechanisms.

- DP.Change_Control_Users: Notification of data content changes
  Notify user of the time and date of the last modification of data.
  This detailed policy statement is addressed by:

  1. O.Change_Control_Users: User notification of data content changes
     Notify users of changes to data content in order to make any adjustments to their own data.

- DP.Config_Mgt_Plan: Implement operational configuration management
  A configuration management plan shall be implemented by the system. The system shall implement configuration management to assure storage integrity, identification of system connectivity (software, hardware, and firmware), and identification of system components (software, hardware, and firmware).
  The system shall implement strong integrity mechanisms (integrity locks, encryption).
  This detailed policy statement is addressed by:

  1. O.Config_Management: Implement operational configuration management
     Implement a configuration management plan. Implement configuration management to assure storage integrity, identification of system connectivity (software, hardware, and firmware), and identification of system components (software, hardware, and firmware).

- DP.Documented_Recovery: Documented recovery
  The system shall provide procedures and features to assure that system recovery is done in a trusted and secure manner. Any circumstances that could result in an untrusted recovery shall be documented.
  This detailed policy statement is addressed by:

  1. O.Trusted_Recovery_Doc: Documentation of untrusted data recovery
     Provide trusted recovery to ensure that data cannot be lost or misplaced. Any circumstances which can cause untrusted recovery to be documented with mitigating procedures established.

- DP.Integrity_Data/SW: Strong integrity mechanisms
  The system shall implement strong integrity mechanisms (integrity locks, encryption).
  This detailed policy statement is addressed by:

  1. O.Integrity_Data/SW: Integrity **protection** for user data and software
     Provide integrity **protection** for user data and software.

- DP.Integrity_Practice: Operational integrity system function testing
  Provide system functional tests to periodically test the integrity of the hardware and code running system functions.
  This detailed policy statement is addressed by:

  1. O.Integrity_Practice: Operational integrity system function testing
     Provide system functional tests to periodically test the integrity of the hardware and code running system functions.

- DP.Malicious_Code: Malicious code prevention
  Procedures and mechanisms to prevent the introduction of malicious code into the system shall be provided.
  This detailed policy statement is addressed by:

  1. O.Malicious_Code: Procedures for preventing malicious code
     Incorporate malicious code prevention procedures and mechanisms.

- DP.Storage_Integrity: Assurance of effective storage integrity
  The system shall provide assurance that storage integrity is effective.
  This detailed policy statement is addressed by:

  1. O.Storage_Integrity: Storage integrity
     Provide integrity for data.

- DP.Sys_Assur_HW/SW/FW: Validation of security function integrity
  Features and procedures to validate the integrity and the expected operation of the security-relevant software, hardware, and firmware shall be provided by the system.

This detailed policy statement is addressed by:

1. O.Sys_Assur_HW/SW/FW: Validation of security function
   Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures.

- DP.System_Protection: **Protection** from security function modification
  Provide features or procedures for **protection** of the system from improper changes.
  This detailed policy statement is addressed by:

  1. O.Config_Management: Implement operational configuration management
     Implement a configuration management plan. Implement configuration management to assure storage integrity, identification of system connectivity (software, hardware, and firmware), and identification of system components (software, hardware, and firmware).

  2. O.Sys_Self_Protection: **Protection** of system security function
     Protect the system security functions through technical features.

- DP.System_Recovery: Trusted system recovery

- DP.System_Recovery: Trusted system recovery
  Provide procedures and features to assure that system recovery is done in a trusted and secure manner.
  This detailed policy statement is addressed by:

  1. O.Trusted_Recovery_Doc: Documentation of untrusted data recovery
     Provide trusted recovery to ensure that data cannot be lost or misplaced. Any circumstances which can cause untrusted recovery to be documented with mitigating procedures established.

- DP.User_Data_Storage: **Protection** of stored user data
  The system shall provide appropriate storage, continuous personnel access control storage, or encrypted storage of data based on the sensitivity of the data.
  Safeguard Application: O.User_Data_Integrity covers part of this policy, but

  an additional objective dealing with confidentiality may be needed.
  This detailed policy statement is addressed by:

  1. O.User_Data_Integrity: Integrity **protection** of stored user data
     Provide appropriate integrity **protection** for stored user data.

  2. O.User_Defined_AC: User-defined access control
     Enforce an access control policy whereby users may determine who may access information they control.

- DP.User_Data_Transfer: **Protection** of transmitted user data
  The system shall provide a protected distribution system for data transmitted.
  This detailed policy statement is addressed by:

  1. O.User_Data_Transfer: **Protection** of transmitted user data
     Provide the ability to have physically protected communications lines, intrusion detection for communications lines, and/or need-to-know isolation for communications lines.

isolation for communications lines.

P.Lifecycle: System lifecycle phases integrate security
Information systems security shall be an integral part of all system lifecycle phases.

In General, P.Lifecycle is addressed by:

1. O.Lifecycle_Security: Lifecycle security
   Provide tools, techniques, and security employed during the development phase. Detect and resolve flaws during the operational phase. Provide safe destruction techniques.

P.Marking: Information marking
Information shall be appropriately marked and labeled.

Example detailed policy statements:

- DP.Config_Mgt_Plan: Implement operational configuration management
  A configuration management plan shall be implemented by the system. The system shall implement configuration management to assure storage integrity, identification of system connectivity (software, hardware, and firmware), and identification of system components (software, hardware, and firmware).
  The system shall implement strong integrity mechanisms (integrity locks, encryption).
  This detailed policy statement is addressed by:

  1. O.Config_Management: Implement operational configuration management
     Implement a configuration management plan. Implement configuration management to assure storage integrity, identification of system connectivity (software, hardware, and firmware), and identification of system components (software, hardware, and firmware).

In General, P.Marking is addressed by:

1. O.External_Labels: Label or mark information for external systems
   Label or mark information for external systems to prevent the exchange of inappropriate data between systems.

TCPA Security Policy

P.MessageAuth: Message authorization
Each message to a TPM protected capability uses the authorization protocol
Coverage Rationale: TCPA specification

In General, P.MessageAuth is addressed by:

1. O.SpecRef: Specification reference
   The TOE must provide all of the features and functions as specified in the TCPA specification.
2. O.MessageAuthentication: Message authentication
   Each requestor must prove knowledge of the shared secret.

P.Physical_Control: Physical **protection**
Information shall be physically protected to prevent unauthorized disclosure, destruction, or modification.

In General, P.Physical_Control is addressed by:

1. O.Tamper_ID: Tamper detection
   Provide system features that detect physical tampering of a system component, and use those features to limit security breaches.

P.SpecRef: Specification reference
The TOE must provide all features and functions of the TCPA in a consistent manner.

In General, P.SpecRef is addressed by:

1. O.SpecRef: Specification reference
   The TOE must provide all of the features and functions as specified in the TCPA specification.
2. O.AuditLog: Audit Log
   The TPS shall maintain the audit log
3. O.RootMeasurement: Measurement root of trust
   The entity that provides the base for measuring integrity values is the measurement root of trust. This entity on a PC would be the boot block or something similar.
4. O.RootReporting: Reporting root of trust

4. O.RootReporting: Reporting root of trust

   The reporting root of trust is the endorsement **key**. This provides a singular point that all challengers can rely on.

5. O.SecureManufacturing: Secure TPM creation and certification

   The TPM manufacturing process requires the creation and certification of the endorsement **key**. The TPM manufacturing process must perform this creation and certification in a manner that provides the assurances that the endorsement **key** was properly created. The process must also provide assurances that the

certification of the endorsement **key** is done with the correct private **key** and that the process protects the certfication **key** and properly protects certfication process.

P.TCPAAuthorization: TCPA Authorization
The TOE must provide the ability to participate in the authorization protocol from chapter 4.
Coverage Rationale: Required by TCPA specification

In General, P.TCPAAuthorization is addressed by:

1. O.SpecRef: Specification reference

   The TOE must provide all of the features and functions as specified in the TCPA specification.

2. O.MetricReporting: Integrity metric reporting

   The TOE must report the values in the current PCR registers. The report may be digitally signed.

3. O.TCPAProtectedStorage: TCPA Protective Storage

   The TOE must provide a protected storage mechanism as defined in the specification section 3.6 and chapter 6.

P.TCPAIdentities: TCPA Identities
The TOE must create and manage identities.
Coverage Rationale: TCPA specification

In General, P.TCPAIdentities is addressed by:

1. O.TCPAIdentities: TCPA Identities
   The TOE must provide the ability to create, manage and use identities.
2. O.TCPAProtectedStorage: TCPA Protective Storage
   The TOE must provide a protected storage mechanism as defined in the specification section 3.6 and chapter 6.

P.TCPAOwnership: TCPA TPM and entity ownership
The TOE must provide the mechanisms to create and use the ownership protocol.
Coverage Rationale: TCPA specification

In General, P.TCPAOwnership is addressed by:

1. O.SpecRef: Specification reference
   The TOE must provide all of the features and functions as specified in the TCPA specification.

---

2. O.TCPAProtectedStorage: TCPA Protective Storage
   The TOE must provide a protected storage mechanism as defined in the specification section 3.6 and chapter 6.

P.TCPAProtectMigrate: TCPA Protected storage **migration** and non **migration**
The TOE must provide the mechanisms to identity the **tree** a storage entity is in (**migratable** or non-**migratable**), ensure that the label once set never changes and manage the **migration**, backup and recovery of storage entities.
Coverage Rationale: TCPA specification

In General, P.TCPAProtectMigrate is addressed by:

1. O.TCPAProtectedStorage: TCPA Protective Storage
   The TOE must provide a protected storage mechanism as defined in the specification section 3.6 and chapter 6.

P.TCPARegDIR: TCPA DIR registers
The TOE must supply DIR registers.
Coverage Rationale: TCPA specification

In General, P.TCPARegDIR is addressed by:

1. O.SpecRef: Specification reference
   The TOE must provide all of the features and functions as specified in the TCPA specification.
2. O.TCPAProtectedStorage: TCPA Protective Storage
   The TOE must provide a protected storage mechanism as defined in the specification section 3.6 and chapter 6.

P.TCPARegPCR: TCPA PCR registers
The TOE must provide volatile PCR registers
Coverage Rationale: TCPA specification

In General, P.TCPARegPCR is addressed by:

1. O.SpecRef: Specification reference
   The TOE must provide all of the features and functions as specified in the TCPA specification.
2. O.MetricReporting: Integrity metric reporting
   The TOE must report the values in the current PCR registers. The report may be digitally signed.

3. O.TCPAProtectedStorage: TCPA Protective Storage
   The TOE must provide a protected storage mechanism as defined in the specification section 3.6 and chapter 6.

P.TSP: TOE Security Policy
A TOE security policy (TSP) must identify all roles, services and security relevant data items, and specify what access (if any) a user, performing a service within the context of a given role, has to each of the secuiryt-relevant data items. The policy must specify that: users agree to protect keys and data access, users agree to report loss of keys or perceived compromise to security and user agree not to collude.

In General, P.TSP is addressed by:

1. O.SpecRef: Specification reference
   The TOE must provide all of the features and functions as specified in the TCPA specification.
2. Security Objectives:

6.2.2 - Threats

T.Admin_Err_Commit: Administrative errors of commission
An administrator commits errors that directly compromise organizational security objectives or change the technical security policy enforced by the system or application.

Example Attacks:

- DA.Adm_Err_Crypto: Accidental mismanagement of cryptographic functions
  An administrator misconfigures cryptographic functions or stores plaintext keys in insecure areas.
  This Attack is addressed by:

  1. O.Crypto_Key_Man: Cryptographic **Key** Management
     Fully define cryptographic components, functions, and interfaces. Ensure appropriate **protection** for cryptographic keys throughout their lifecycle, covering generation, distribution, storage, use, and destruction.

- DA.Admin_Err_AC_Policy: Administrator error modifies access control or information flow policy
  An administrator's error in data entry changes the access control or information flow policy enforced by the system in such a way that it no longer serves its

intended purpose.
This Attack is addressed by:

1. O.Admin_Guidance: Administrator guidance documentation
   Deter administrator errors by providing adequate administrator guidance.

Objective Component Application: Administrator guidance shall

address administrator errors that change the access control or information flow policy enforced by the system or application in such a way that it no longer serves its intended purpose.

- DA.Admin_Err_Audit: Administrator error changes audit behavior
  An administrator's error in data entry changes the audit behavior of the system in such a way that auditing no longer serves its intended purpose.
  This Attack is addressed by:

  1. O.Admin_Guidance: Administrator guidance documentation
     Deter administrator errors by providing adequate administrator guidance.
     Objective Component Application: Administrator guidance shall

     address errors that change the audit policy enforced by the TSF.

In General, T.Admin_Err_Commit is addressed by:

1. O.Audit_Protect: Protect stored audit records
   Protect audit records against unauthorized access, modification, or deletion to ensure accountability of user actions.
2. O.Security_Attr_Mgt: Manage security attributes
   Manage the initialization of, values for, and allowable operations on security attributes.
3. O.Security_Data_Mgt: Manage security-critical data
   Manage the initialization of, limits on, and allowable operations on security-critical data.

critical data.

4. O.Security_Func_Mgt: Manage behavior of security functions
   Provide management mechanisms for security mechanisms.
5. O.Security_Roles: Security roles
   Maintain security-relevant roles and the association of users with those roles.
6. O.Limit_Actions_Auth: Restrict actions before authentication
   Restrict the actions a user may perform before the TOE verifies the identity of the user.

T.Admin_Err_Omit: Administrative errors of omission
The system administrator fails to perform some function essential to security.

Example Attacks:

- DA.Adm_Err_Crypto: Accidental mismanagement of cryptographic functions
  An administrator misconfigures cryptographic functions or stores plaintext keys in insecure areas.
  This Attack is addressed by:

TCPA Security Policy

1. O.Crypto_Key_Man: Cryptographic **Key** Management
   Fully define cryptographic components, functions, and interfaces. Ensure appropriate **protection** for cryptographic keys throughout their lifecycle, covering generation, distribution, storage, use, and destruction.

In General, T.Admin_Err_Omit is addressed by:

1. O.Admin_Guidance: Administrator guidance documentation
   Deter administrator errors by providing adequate administrator guidance.
2. O.User_Auth_Management: User authorization management
   Manage and update user authorization and privilege data in accordance with organizational security and personnel policies.

T.Admin_UserPriv: Administrator violates user privacy policy

An administrator learns the identity (or other privacy related information) of user(s) in violation of user privacy policy. Privacy-related information is sensitive information associated with the identity of a user.

In General, T.Admin_UserPriv is addressed by:

1. O.Prevent_Link: Prevent linking of multiple service use
   Ensure that a user may make multiple uses of a service or resource without other specified users being able to link these uses together.

T.Component_Failure: A critical system component fails
Failure of one or more system components results in the loss of system-critical functionality.

In General, T.Component_Failure is addressed by:

1. O.Crypto_Key_Man: Cryptographic **Key** Management
   Fully define cryptographic components, functions, and interfaces. Ensure appropriate **protection** for cryptographic keys throughout their lifecycle, covering generation, distribution, storage, use, and destruction.
2. O.Crypto_Data_Sep: Separation of cryptographic data
   Provide complete separation between plaintext and encrypted data and between data and keys. This requires separate channels and separate storage areas. The only place any data can pass between the plaintext and encrypted data modules is in the cryptographic engine. There should be no way for plaintext keys to reach either data module and no way for data to enter the **key** handling module. Eencrypted keys can be handled as encrypted data, but with limited user access.
3. O.Crypto_Dsgn_Impl: Cryptographic Design and Implementation
   Minimize or even eliminate design and implementation errors in the cryptographic modules and functions.
4. O.Crypto_Modular_Dsgn: Cryptographic Modular Design
   Prevent errors in one part of the TOE from influencing other parts, especially

cryptographic parts. To this end, noncryptographic I/O paths must be well defined and logically independent of circuitry and processes performing **key** generation, manual **key** entry, **key** zeroising, and similar **key**-related operations.

5. O.Crypto_Operation: Cryptographic function definition
   Cryptographic components, functions, and interfaces shall be fully defined.
6. O.Crypto_Self_Test: Cryptographic self test
   Provide the ability to verify that the cryptographic functions operate as designed.
7. O.Crypto_Test_Reqs: Test cryptographic functionality
   Test cryptographic operation and **key** management.
8. O.Fail_Secure: Preservation of secure state for failures in critical components
   Preserve the secure state of the system in the event of a secure component failure.
9. O.Fault_Tolerance: Provide fault tolerant operations for critical components
   Provide fault tolerant operations for critical components and continue to operate in the presence of specific failures in one or more system components.
10. O.Secure_State: Protect and maintain secure system state
    Maintain and recover to a secure state without security compromise after system error or other interruption of system operation.

T.Dev_Flawed_Code: Software containing security-related flaws
A system or applications developer delivers code that does not perform according to specifications or contains security flaws.

In General, T.Dev_Flawed_Code is addressed by:

1. O.Code_Signing: Code signing and verification
   Check verification of signed downloaded code prior to execution. A well-known example is checking digital signatures on signed Java applets.
2. O.Integ_Sys_Data_Int: Integrity of system data transferred internally
   Ensure the integrity of system data transferred internally.
3. O.No_Residual_Info: Eliminate residual information
   Ensure there is no "object reuse;" i.e., ensure that there is no residual information in some information containers or system resources upon their reallocation to different users.
4. O.Secure_State: Protect and maintain secure system state
   Maintain and recover to a secure state without security compromise after system error or other interruption of system operation.
5. O.Sys_Self_Protection: **Protection** of system security function
   Protect the system security functions through technical features.
6. O.Integ_Sys_Data_Ext: Integrity of system data transferred externally
   Ensure the integrity of system data exchanged externally with another trusted product by using a protocol for data transfer that will permit error detection and correction.
   This includes detecting and possibly correcting errors in data received and

encoding outgoing data to make it possible for the receiver to detect and possibly

correct errors. The method for detecting and correcting errors is based on some method (protocol) that is agreed upon by participating parties.

7. O.Source_Code_Exam: Examine the source code for developer flaws
   Examine for accidental or deliberate flaws in code made by the developer. The accidental flaws could be lack of engineering detail or bad design. Where the deliberate flaws would include building trapdoors for later entry as an example.

T.EndorseExpose: Exposure of endorsement **key**
The endorsement **key** provides the root of reporting trust. If exposed it provides the attacker numerous mechanisms that allow for the forgery, cloning and masquerading as a valid TPM

In General, T.EndorseExpose is addressed by:

1. O.NoBore: No BORE attacks
   The TOE provides **protection** from Break Once Run Everywhere attacks.
2. O.Protected_Capability: Protected Capability and shielded location
   The TOE must identity and protect capabilities as defined in the TCPA specification.
3. O.SpecRef: Specification reference
   The TOE must provide all of the features and functions as specified in the TCPA specification.
4. O.TCPAIdentities: TCPA Identities
   The TOE must provide the ability to create, manage and use identities.
5. O.RootReporting: Reporting root of trust
   The reporting root of trust is the endorsement **key**. This provides a singular point that all challengers can rely on.
6. O.Admin_Guidance: Administrator guidance documentation
   Deter administrator errors by providing adequate administrator guidance.
7. O.Code_Signing: Code signing and verification
   Check verification of signed downloaded code prior to execution. A well-known

Check verification of signed downloaded code prior to execution. A well-known example is checking digital signatures on signed Java applets.

8. O.Crypto_Data_Sep: Separation of cryptographic data
   Provide complete separation between plaintext and encrypted data and between data and keys. This requires separate channels and separate storage areas. The only place any data can pass between the plaintext and encrypted data modules is in the cryptographic engine. There should be no way for plaintext keys to reach either data module and no way for data to enter the **key** handling module. Eencrypted keys can be handled as encrypted data, but with limited user access.
9. O.Crypto_Dsgn_Impl: Cryptographic Design and Implementation
   Minimize or even eliminate design and implementation errors in the cryptographic modules and functions.
10. O.Crypto_Key_Man: Cryptographic **Key** Management
    Fully define cryptographic components, functions, and interfaces. Ensure appropriate **protection** for cryptographic keys throughout their lifecycle, covering generation, distribution, storage, use, and destruction.

---

11. O.Fault_Tolerance: Provide fault tolerant operations for critical components
    Provide fault tolerant operations for critical components and continue to operate in the presence of specific failures in one or more system components.
12. O.Fail_Secure: Preservation of secure state for failures in critical components
    Preserve the secure state of the system in the event of a secure component failure.
13. O.Integ_Sys_Data_Ext: Integrity of system data transferred externally
    Ensure the integrity of system data exchanged externally with another trusted product by using a protocol for data transfer that will permit error detection and correction.
    This includes detecting and possibly correcting errors in data received and

    encoding outgoing data to make it possible for the receiver to detect and possibly correct errors. The method for detecting and correcting errors is based on some method (protocol) that is agreed upon by participating parties.
14. O.Integ_Sys_Data_Int: Integrity of system data transferred internally
    Ensure the integrity of system data transferred internally.
15. O.MetricReporting: Integrity metric reporting

The TOE must report the values in the current PCR registers. The report may be digitally signed.

16. O.EMSEC_Design: Provide physical emanations security
    Design and build the system in such a way as to control the production of intelligible emanations within specified limits.
17. O.Trusted_Recovery_Doc: Documentation of untrusted data recovery
    Provide trusted recovery to ensure that data cannot be lost or misplaced. Any circumstances which can cause untrusted recovery to be documented with mitigating procedures established.
18. O.Trusted_Recovery: Trusted recovery of security functionality
    Recovery to a secure state, without security compromise, after a discontinuity of operations.

T.Failure_DS_Comp: Failure of a distributed system component
Failure of a component that is part of a distributed system will cause other parts of the distributed system to malfunction or provide unreliable results.

In General, T.Failure_DS_Comp is addressed by:

1. O.Fault_Tolerance: Provide fault tolerant operations for critical components
   Provide fault tolerant operations for critical components and continue to operate in the presence of specific failures in one or more system components.
2. O.Integrity_Data_Rep: Integrity of system data replication
   Ensure that when system data replication occurs across the system the data is consistent for each replication.

T.GlobalSecret: Global secret exposure
If the TOE has a global secret known to all TOE's then exposure of one TOE exposes all TOE's.

Coverage Rationale: This threat creates a system then when broken breaks all systems,

avoidance of this situation is normally a good design.

In General, T.GlobalSecret is addressed by:

1. O.NoBore: No BORE attacks
   The TOE provides **protection** from Break Once Run Everywhere attacks.
2. O.Crypto_Dsgn_Impl: Cryptographic Design and Implementation
   Minimize or even eliminate design and implementation errors in the cryptographic modules and functions.

T.Hack_AC: Hacker undetected system access
A hacker gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.

In General, T.Hack_AC is addressed by:

1. O.Trusted_Path: Provide a trusted path
   Provide a trusted path between the user and the system. Execution of a user-requested action must be made via a trusted path with the following properties:
   * The path is logically distinct from, and cannot be confused with other communication paths (by either the user or the system).
   * The path provides assured identification of its end points.
2. O.Apply_Code_Fixes: Apply patches to fix the code
   Apply patches to fix the code when vulnerabilities in code allow unauthorized and undiscovered access.
3. O.AuditLog: Audit Log
   The TPS shall maintain the audit log

T.Hack_Avl_Resource: Hacker attempts resource denial of service
A hacker executes commands, sends data, or performs other operations that make system resources unavailable to system users. Resources that may be denied to users include bandwidth, processor time, memory, and data storage.

In General, T.Hack_Avl_Resource is addressed by:

1. O.Audit_Generation: Audit records with identity
   Record in audit records: date and time of action, location of the action, and the entity responsible for the action.
2. O.Hack_Limit_Sessions: Limit sessions to outside users
   Limit the number of sessions available to outside users. A hacker can initiate multiple communication sessions that could cause an overload on resources, for example, half open session starts as is seen in "SYN flood" attacks.

3. O.Manage_TSF_Data: Manage security-critical data to avoid storage space being exceeded
   Manage security-critical (TSF) data to ensure that the size of the data does not exceed the space allocated for storage of the data.
4. O.React_Discovered_Atk: React to discovered attacks
   Implement automated notification or other reactions to the TSF-discovered attacks in an effort to identify attacks and to create an attack deterrent.
5. O.Data_Imp_Exp_Control: Data import/export to/from system control
   Protect data from being sent to erroneous places and more places external to the system than allowed by the organization's security policy. Conversely the import of data into the system should be protected from illicit information or information not allowed by the organization's security policy.
6. O.AuditLog: Audit Log
   The TPS shall maintain the audit log

T.Hack_Comm_Eavesdrop: Hacker eavesdrops on user data communications
Hacker obtains user data by eavesdropping on communications lines.

In General, T.Hack_Comm_Eavesdrop is addressed by:

1. O.Data_Exchange_Conf: Enforce data exchange confidentiality
   Protect user data confidentiality when exchanging data with a remote system.

T.Hack_Crypto: Cryptoanalysis for theft of information
A hacker performs cryptoanalysis on encrypted data in order to recover message content.

In General, T.Hack_Crypto is addressed by:

1. O.Crypto_Data_Sep: Separation of cryptographic data
   Provide complete separation between plaintext and encrypted data and between data and keys. This requires separate channels and separate storage areas. The only place any data can pass between the plaintext and encrypted data modules is in the cryptographic engine. There should be no way for plaintext keys to reach either data module and no way for data to enter the key handling module.

either data module and no way for data to enter the **key** handling module. Eencrypted keys can be handled as encrypted data, but with limited user access.

2. O.EMSEC_Design: Provide physical emanations security
   Design and build the system in such a way as to control the production of intelligible emanations within specified limits.
3. O.IntelEman_Control: Emanations control
   Limit system-produced intelligible emanations to within a specified limit.
4. O.IntelEman_Contain: Emanations containment
   Confine system-produced intelligible emanations to within a specified limit.
5. O.SpecRef: Specification reference
   The TOE must provide all of the features and functions as specified in the TCPA specification.

6. O.Protected_Capability: Protected Capability and shielded location
   The TOE must identity and protect capabilities as defined in the TCPA specification.

T.Hack_Msg_Data: Message content modification
A hacker modifies information intercepted from a communication link between two unsuspecting entities before passing it on, thereby deceiving the intended recipient.

In General, T.Hack_Msg_Data is addressed by:

1. O.Rcv_MsgMod_ID: Identify message modification in messages received
   The TSF recognizes changes to messages that occurred in transit, including insertion of spurious messages and deletion or replay of legitimate messages.
2. O.Snt_MsgMod_ID: Identify message modification in messages sent
   The TSF supports recognition of changes to transmitted messages that occurred in transit, including insertion of spurious messages and deletion or replay of legitimate messages.
3. O.TSF_Rcv_Err_ID_Loc: Local detection of received security-critical data modified in transit
   Identification by the system (TOE) of modification of security-critical (TSF) data

occurring in transit from a remote trusted site must occur.

4. O.TSF_Rcv_Err_ID_Rem: Remote detection of received security-critical data modified in transit
   Identification by the remote site of the modification of security-critical (TSF) data occurring in transit from the remote site must occur.
5. O.TSF_Snd_Err_ID_Loc: Local detection of sent security-critical data modified in transit
   Identification of modification of security-critical (TSF) data occurring in transit to a remote site by the TSF must occur.
6. O.TSF_Snd_Err_ID_Rem: Remote detection of sent security-critical data modified in transit.
   Identification of modification of security-critical (TSF) data occurring in transit to a remote site by the remote site must occur.
7. O.AuditLog: Audit Log
   The TPS shall maintain the audit log

T.Hack_Phys: Exploitation of vulnerabilities in the physical environment of the system
A hacker physically interacts with the system to exploit vulnerabilities in the physical environment, resulting in arbitrary security compromises.

In General, T.Hack_Phys is addressed by:

1. O.EMSEC_Design: Provide physical emanations security
   Design and build the system in such a way as to control the production of intelligible emanations within specified limits.

2. O.Tamper_ID: Tamper detection
   Provide system features that detect physical tampering of a system component, and use those features to limit security breaches.
3. O.Tamper_Resistance: Tamper resistance
   Prevent or resist physical tampering with specified system devices and components.
4. O.IntelEman_Contain: Emanations containment

4. O.IntelEman_Contain: Emanations containment
   Confine system-produced intelligible emanations to within a specified limit.
5. O.IntelEman_Control: Emanations control
   Limit system-produced intelligible emanations to within a specified limit.

T.Hack_Social_Engineer: Social engineering
A hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation.

In General, T.Hack_Social_Engineer is addressed by:

1. O.Admin_Guidance: Administrator guidance documentation
   Deter administrator errors by providing adequate administrator guidance.
2. O.User_Guidance: User guidance documentation
   Provide documentation for the general user.

T.IdenClone: Identity cloning
Identities are unique keys that must remain protected by the TPM. Creating a copy of the identity breaks the uniqueness promise.

In General, T.IdenClone is addressed by:

1. O.TCPAIdentities: TCPA Identities
   The TOE must provide the ability to create, manage and use identities.
2. O.RootReporting: Reporting root of trust
   The reporting root of trust is the endorsement **key**. This provides a singular point that all challengers can rely on.
3. O.Crypto_Data_Sep: Separation of cryptographic data
   Provide complete separation between plaintext and encrypted data and between data and keys. This requires separate channels and separate storage areas. The only place any data can pass between the plaintext and encrypted data modules is in the cryptographic engine. There should be no way for plaintext keys to reach either data module and no way for data to enter the **key** handling module. Eencrypted keys can be handled as encrypted data, but with limited user access.
4. O.Export_Control: Sanitize data objects containing hidden or unused data
   Sanitize data objects that may contain hidden data when they are exported from the TOE in order to inhibit steganographic smuggling.
5. O.External_Labels: Label or mark information for external systems
   Label or mark information for external systems to prevent the exchange of inappropriate data between systems.

6. O.Integ_User_Data_Int: Protect user data during internal transfer
   Ensure the integrity of user data transferred internally within the system.
7. O.MetricReporting: Integrity metric reporting
   The TOE must report the values in the current PCR registers. The report may be digitally signed.

T.IdenPKI: Identity PKI
The identity creation process requires a PKI to certify the identity. This PKI must ensure the uniqueness of the identity and validate the endorsement **key**. Failure to properly perform these operations results in a bad identity.

In General, T.IdenPKI is addressed by:

1. O.TCPAIdentities: TCPA Identities
   The TOE must provide the ability to create, manage and use identities.
2. O.RootReporting: Reporting root of trust
   The reporting root of trust is the endorsement **key**. This provides a singular point that all challengers can rely on.
3. O.MetricReporting: Integrity metric reporting
   The TOE must report the values in the current PCR registers. The report may be digitally signed.

T.Malicious_Code: Malicious code exploitation
An authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of system assets.
Coverage Rationale: An authorized user, IT system, or hacker downloads an object

either deliberately or accidentally. The user does this primarily in order to gain assets that will assist in their job performance. The IT system may do this to meet informational requirements. The hacker may do this in an effort to satisfy destructive goals. The malicious code is then executed via a trigger mechanism. The trigger mechanism can be executed automatically after download, manually by the hacker, or unknowingly by the authorized user. The results of the attack affect the target system or any other system that the target system can influence.

In General, T.Malicious_Code is addressed by:

In General, T.Malicious_Code is addressed by:

1. O.Trusted_Path: Provide a trusted path

   Provide a trusted path between the user and the system. Execution of a user-requested action must be made via a trusted path with the following properties:

   * The path is logically distinct from, and cannot be confused with other communication paths (by either the user or the system).

   * The path provides assured identification of its end points.

2. O.Admin_Code_Val: Administrative validation of executables

   Validate executable objects prior to allowing execution. Validation needs to be

   done by someone with an expertise to recognize malicious code and the authority and means to prevent its execution.

3. O.Clean_Obj_Recovery: Object and data recovery free from malicious code

   Recover to a viable state after malicious code is introduced and damage occurs, removing the malicious code as part of the process.

4. O.Code_Signing: Code signing and verification

   Check verification of signed downloaded code prior to execution. A well-known example is checking digital signatures on signed Java applets.

5. O.General_Integ_Checks: Periodically check integrity

   Provide periodic integrity checks on both system and user data.

6. O.Obj_Protection: Object domain **protection**

   Require domain **protection** for objects. Specify object classes (domains), user groups, and operation classes. Use these to specify which operations may be performed on which objects by which users. Basically this controls what users can do in a given group.

7. O.Input_Inspection: Require inspection for absence of malicious code.

   Require inspection of downloads/transfers.

8. O.AuditLog: Audit Log

   The TPS shall maintain the audit log

T.MeasureFalse: False integrity measurement

The entity or process providing the integrity measurement provides a false value.

In General, T.MeasureFalse is addressed by:

1. O.RootMeasurement: Measurement root of trust
   The entity that provides the base for measuring integrity values is the measurement root of trust. This entity on a PC would be the boot block or something similar.

T.OwnerMasquerade: Owner masquerade
At attacker can masquerade as the owner of either the TPM or an entity if they obtain the owner authorization data.

In General, T.OwnerMasquerade is addressed by:

1. O.SpecRef: Specification reference
   The TOE must provide all of the features and functions as specified in the TCPA specification.
2. O.TCPAIdentities: TCPA Identities
   The TOE must provide the ability to create, manage and use identities.
3. O.TCPAProtectedStorage: TCPA Protective Storage
   The TOE must provide a protected storage mechanism as defined in the specification section 3.6 and chapter 6.
4. O.Crypto_Data_Sep: Separation of cryptographic data
   Provide complete separation between plaintext and encrypted data and between

   data and keys. This requires separate channels and separate storage areas. The only place any data can pass between the plaintext and encrypted data modules is in the cryptographic engine. There should be no way for plaintext keys to reach either data module and no way for data to enter the **key** handling module. Eencrypted keys can be handled as encrypted data, but with limited user access.
5. O.Crypto_Dsgn_Impl: Cryptographic Design and Implementation
   Minimize or even eliminate design and implementation errors in the cryptographic modules and functions.
6. O.User_Auth_Management: User authorization management
   Manage and update user authorization and privilege data in accordance with

Manage and update user authorization and privilege data in accordance with organizational security and personnel policies.

7. O.User_Conf_Prevention: Basic confidentiality-breach prevention
   Prevent unauthorized export of confidential information from the TOE with moderate effectiveness.

T.Power_Disrupt: Unexpected disruption of system or component power
A human or environmental agent disrupts power causing the system to lose information or security **protection**.

In General, T.Power_Disrupt is addressed by:

1. O.Atomic_Functions: Complete security functions or recover to previous state
   Recover automatically to a consistent, secure state if a security function does not complete successfully in the presence of certain types of failures.
2. O.Trusted_Recovery: Trusted recovery of security functionality
   Recovery to a secure state, without security compromise, after a discontinuity of operations.

T.ProtStorAttribute: Protected storage attribute
Each protected storage object has attributes that indicate it's **migration** status, object type and source. Modification of these attributes allows the attacker to use the object in an unauthorized manner.

In General, T.ProtStorAttribute is addressed by:

1. O.Protected_Capability: Protected Capability and shielded location
   The TOE must identity and protect capabilities as defined in the TCPA specification.
2. O.TCPAProtectedStorage: TCPA Protective Storage
   The TOE must provide a protected storage mechanism as defined in the specification section 3.6 and chapter 6.
3. O.Crypto_Data_Sep: Separation of cryptographic data
   Provide complete separation between plaintext and encrypted data and between data and keys. This requires separate channels and separate storage areas. The only place any data can pass between the plaintext and encrypted data modules is in the cryptographic engine. There should be no way for plaintext keys to reach

either data module and no way for data to enter the **key** handling module. Eencrypted keys can be handled as encrypted data, but with limited user access.

4. O.Data_Exchange_Conf: Enforce data exchange confidentiality
   Protect user data confidentiality when exchanging data with a remote system.
5. O.External_Labels: Label or mark information for external systems
   Label or mark information for external systems to prevent the exchange of inappropriate data between systems.
6. O.Integ_Data_Mark_Exp: Data marking integrity export
   Ensure that data markings are included with data that is exported to another trusted product.
7. O.Integ_User_Data_Int: Protect user data during internal transfer
   Ensure the integrity of user data transferred internally within the system.
8. O.Integrity_Data/SW: Integrity **protection** for user data and software
   Provide integrity **protection** for user data and software.
9. O.User_Data_Integrity: Integrity **protection** of stored user data
   Provide appropriate integrity **protection** for stored user data.

T.ProtStoreBackup: Protected storage backup
The protected storage backup mechanism must provide assurances that the **migration** and non-**migration** bits are properly followed. If they are not followed then non-**migratable** information may move from one system to another.
Coverage Rationale: The backup process can allow the transfer of information from

one TPM to another if the **migration** status is not properly followed.

In General, T.ProtStoreBackup is addressed by:

1. O.TCPAProtectedStorage: TCPA Protective Storage
   The TOE must provide a protected storage mechanism as defined in the specification section 3.6 and chapter 6.
2. O.TCPAIdentities: TCPA Identities
   The TOE must provide the ability to create, manage and use identities.
3. O.Crypto_Dsgn_Impl: Cryptographic Design and Implementation
   Minimize or even eliminate design and implementation errors in the cryptographic modules and functions.
4. O.Export_Control: Sanitize data objects containing hidden or unused data
   Sanitize data objects that may contain hidden data when they are exported from the TOE in order to inhibit steganographic smuggling.
5. O.External_Labels: Label or mark information for external systems
   Label or mark information for external systems to prevent the exchange of

Label or mark information for external systems to prevent the exchange of inappropriate data between systems.

6. O.Integ_Data_Mark_Exp: Data marking integrity export
   Ensure that data markings are included with data that is exported to another trusted product.
7. O.Trusted_Recovery_Doc: Documentation of untrusted data recovery
   Provide trusted recovery to ensure that data cannot be lost or misplaced. Any

circumstances which can cause untrusted recovery to be documented with mitigating procedures established.

8. O.Trusted_Recovery: Trusted recovery of security functionality
   Recovery to a secure state, without security compromise, after a discontinuity of operations.

T.ProtStoreCrypto: Protected Storage Cryptography
Protected storage requires cryptography to protect the contents when the data is not inside the TPM. Failure of the cryptography exposes the data.
Coverage Rationale: The protected store must provide reasonable protections of the

data using cryptograhpy.

In General, T.ProtStoreCrypto is addressed by:

1. O.Protected_Capability: Protected Capability and shielded location
   The TOE must identity and protect capabilities as defined in the TCPA specification.
2. O.TCPAProtectedStorage: TCPA Protective Storage
   The TOE must provide a protected storage mechanism as defined in the specification section 3.6 and chapter 6.
3. O.Crypto_Data_Sep: Separation of cryptographic data
   Provide complete separation between plaintext and encrypted data and between data and keys. This requires separate channels and separate storage areas. The only place any data can pass between the plaintext and encrypted data modules is in the cryptographic engine. There should be no way for plaintext keys to reach

either data module and no way for data to enter the **key** handling module.
Eencrypted keys can be handled as encrypted data, but with limited user access.

4. O.Crypto_Dsgn_Impl: Cryptographic Design and Implementation
   Minimize or even eliminate design and implementation errors in the cryptographic modules and functions.
5. O.User_Data_Integrity: Integrity **protection** of stored user data
   Provide appropriate integrity **protection** for stored user data.

T.ProtStoreMaintenance: Protected storage maintenance
The protected storage maintenance feature allows for the cloning of a TPM. If this mechanism is abused then the attacker can make copies of TPM devices.
Coverage Rationale: When implemented the maintenance feature must be protected to

eliminate the cloning problem.

In General, T.ProtStoreMaintenance is addressed by:

1. O.TCPAProtectedStorage: TCPA Protective Storage
   The TOE must provide a protected storage mechanism as defined in the specification section 3.6 and chapter 6.

2. O.Protected_Capability: Protected Capability and shielded location
   The TOE must identity and protect capabilities as defined in the TCPA specification.
3. O.TCPAIdentities: TCPA Identities
   The TOE must provide the ability to create, manage and use identities.
4. O.Crypto_Dsgn_Impl: Cryptographic Design and Implementation
   Minimize or even eliminate design and implementation errors in the cryptographic modules and functions.
5. O.Data_Exchange_Conf: Enforce data exchange confidentiality
   Protect user data confidentiality when exchanging data with a remote system.
6. O.Export_Control: Sanitize data objects containing hidden or unused data
   Sanitize data objects that may contain hidden data when they are exported from the TOE in order to inhibit steganographic smuggling.

the TOE in order to inhibit steganographic smuggling.

7. O.External_Labels: Label or mark information for external systems
   Label or mark information for external systems to prevent the exchange of inappropriate data between systems.
8. O.Integ_Data_Mark_Exp: Data marking integrity export
   Ensure that data markings are included with data that is exported to another trusted product.
9. O.Trusted_Recovery_Doc: Documentation of untrusted data recovery
   Provide trusted recovery to ensure that data cannot be lost or misplaced. Any circumstances which can cause untrusted recovery to be documented with mitigating procedures established.
10. O.Trusted_Recovery: Trusted recovery of security functionality
    Recovery to a secure state, without security compromise, after a discontinuity of operations.

T.Repudiate_Receive: Recipient denies receiving information
The recipient of a message denies receiving the message, to avoid accountability for receiving the message or to avoid obligations incurred as a result of receiving the message.

In General, T.Repudiate_Receive is addressed by:

1. O.NonRepud_Assess_Recd: Non-repudiation support for received information by a nonlocal sender's TSF
   Support nonrepudiation for received information by supporting remote handling of nonrepudiation evidence if needed.
2. O.NonRepud_Gen_Recd: Non-repudiation support for received information by the recipient's TSF
   Prevent a receiving user from avoiding accountability for receiving a message by providing evidence that the user received the message.

T.Repudiate_Send: Sender denies sending information
The sender of a message denies sending the message to avoid accountability for sending the message or to avoid obligations incurred as a result of sending the message.

In General, T.Repudiate_Send is addressed by:

1. O.NonRepud_Assess_Sent: Non-repudiation support for sent information by the nonlocal receiving TSF.
   Support nonrepudiation for sent information by supporting remote handling of nonrepudiation evidence if needed.
2. O.NonRepud_Gen_Sent: Non-repudiation support for sent information by the sender's TSF.
   Prevent a user from avoiding accountability for sending a message to a recipient at a different site by providing evidence that the user sent the message.

T.Repudiate_Transact: A participant denies performing a transaction
A participant in a transaction denies participation in the transaction to avoid accountability for the transaction or for resulting obligations.

In General, T.Repudiate_Transact is addressed by:

1. O.NonRepud_Assess_Recd: Non-repudiation support for received information by a nonlocal sender's TSF
   Support nonrepudiation for received information by supporting remote handling of nonrepudiation evidence if needed. <